UMOWA Nr .....

Zawarta w dniu ..... pomiędzy: Miastem Gorzów Wlkp. - Urząd Miasta Gorzowa Wlkp. ul. Sikorskiego 3-4, 66-400 Gorzów Wlkp., NIP 599-00-19-632 reprezentowanym przez: Jacka Wójcickiego - Prezydenta Miasta Gorzowa Wlkp. zwanym w dalszej części umowy „Zamawiającym".
a:
..... zwanym w dalszej części umowy „Wykonawcą".

§ 1
Tryb postępowania poprzedzający zawarcie Umowy

Niniejszą Umowę zawarto z Wykonawcą wyłonionym w postępowaniu o udzielenie zamówienia publicznego przeprowadzonym w trybie przetargu nieograniczonego zgodnie - z przepisami ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2015 r. poz. 2164 ze zm.).

§ 2
Przedmiot Umowy

Przedmiotem niniejszej umowy jest:

1. Dostawa wraz z wdrożeniem platformy serwerowej oraz infrastruktury dla Hurtowni Danych wraz z oprogramowaniem do wirtualizacji oraz oprogramowaniem systemów serwerowych:
   1) Zadanie I
      - Serwery – 5 szt.
      - Macierz typ I – 2 szt.
      - Macierz typ II – 2 szt.
      - Serwerowy system operacyjny – 6 szt.
      - Pakiet licencji dostępowych – 370 szt.
      - System zarządzania środowiskami serwerowymi – 6 szt.
      - Dostawa voucherów dla min. 2 administratorów IT do zrealizowania w autoryzowanym ośrodku szkoleniowym producenta oprogramowania.
   2) Zadanie II
      - Serwer – 1 szt.
      - Pakiet licencji dostępowych – 200 szt.
2. Szczegółowy opis przedmiotu zamówienia został określony w załączniku nr 1 do umowy.
3. Integralną częścią umowy są następujące załączniki:
   - Opis Przedmiotu Zamówienia – załącznik nr 1,
   - Formularz Ofertowy Wykonawcy – załącznik nr 2,
   - Protokół Odbioru (wzór) – załącznik nr 3

4. Zadanie o którym mowa w ust. 1 pkt 1 zostanie wykonane w ramach projektu pn. "Rozwój elektronicznych usług świadczonych przez Urząd Miasta Gorzowa Wlkp. oraz udostępniania danych publicznych". Projekt nr RPLB.02.01.01-08-0040/15, który jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego LUBUSKIE 2020, Oś 2 Rozwój cyfrowy; Działanie 2.1 Rozwój społeczeństwa informacyjnego. Poddziałanie 2.1.1 Rozwój społeczeństwa informacyjnego.

§ 3
Termin realizacji Umowy

Termin wykonania zamówienia – 30 dni roboczych od dnia podpisania niniejszej umowy.

§ 4
Warunki realizacji Umowy

1. Wykonawca dostarczy sprzęt i oprogramowanie na własny koszt i na własne ryzyko na adres: Urząd Miasta Gorzowa Wlkp. ul. Sikorskiego 3-4, 66-400 Gorzów Wlkp.
2. Termin dostawy będzie uzgadniany (jednak nie później niż na 3 dni przed terminem dostawy) z upoważnionym przedstawicielem Zamawiającego, wskazanym w niniejszej Umowie.
3. Dostarczony sprzęt i oprogramowanie będzie oryginalnie opakowany (opakowania nie mogą być naruszone), opakowania opisane, co do ich zawartości oraz oznakowane symbolem CE zgodnie z wymogami określonymi w rozporządzeniu MGPiPSz dnia 21 sierpnia 2007 roku w sprawie zasadniczych wymagań sprzętu elektrycznego (Dz. U. Nr 155, poz. 1089).
4. Dostarczony sprzęt i oprogramowanie zaopatrzone będzie w instrukcję (jeżeli taką instrukcję posiada) opisy techniczne i karty gwarancyjne, które będą w języku polskim.
5. Prawo własności do dostarczonego zgodnie z umową sprzętu i oprogramowania przejdzie na Zamawiającego po podpisaniu Protokołu Odbioru bez uwag (przez osoby wskazane w umowie) i zapłaceniu faktury VAT przez Zamawiającego.

§ 5
Odpowiedzialność Wykonawcy

1. Za wady fizyczne i jakościowe dostarczonego sprzętu i oprogramowania odpowiada Wykonawca.
2. Za działania i zaniechania osób, przy pomocy, których Wykonawca będzie wykonywał zobowiązania zaciągnięte w myśl postanowień niniejszej umowy oraz za szkody w mieniu Zamawiającego, powstałe w związku z realizacją niniejszej umowy Wykonawca zawsze odpowiada, jak za działania i zaniechania własne.
3. Wykonawca oświadcza, iż przedmiot umowy jest fabrycznie nowy, wolny od wad fizycznych i prawnych oraz że przejmuje na siebie wszelką odpowiedzialność z tytułu roszczeń, z jakimi osoby trzecie mogłyby wystąpić przeciwko Zamawiającemu z tytułu korzystania z praw należących do osób trzecich, w szczególności praw autorskich, licencji, patentów, wzorów użytkowych lub znaków towarowych w odniesieniu do przedmiotu umowy, jeżeli normalne użytkowanie przedmiotu umowy wymaga korzystania z tych praw.

§ 6
Odbiór

1. Zamawiający odbierze dostarczony sprzęt i oprogramowanie, sporządzając w tym celu 2 egzemplarze Protokołu Odbioru, podpisanego przez osoby wskazane w niniejszej umowie.

2. Zamawiający sprawdzi dostarczony sprzęt i oprogramowanie w obecności przedstawiciela Wykonawcy w terminie nie dłuższym niż 7 dni roboczych od daty dostawy całości zamówienia, a w przypadku stwierdzenia wad jakościowych, bądź braków ilościowych zgłosi Wykonawcy zastrzeżenia.
3. Wykonawca odbierze sprzęt i oprogramowanie nie spełniające warunków umowy na swój koszt, a w terminie nie dłuższym niż 7 dni od dnia poinformowania go o tym fakcie, dostarczy nieodpłatnie sprzęt i oprogramowanie wolne od wad.
4. W protokole Strony zgłoszą zastrzeżenia odnośnie wad lub braków sprzętu i oprogramowania.

§ 7
Gwarancja i rękojmia

1. Wykonawca gwarantuje najwyższą jakość przedmiotu umowy i udziela Zamawiającemu gwarancji jakości producenta na dostarczony sprzęt i oprogramowanie.
2. Okres gwarancji rozpocznie się od dnia podpisania Protokołu Odbioru jakościowo-ilościowego dostarczonego przedmiotu zamówienia, bez uwag.
3. Jakiekolwiek dokumenty gwarancyjne wydane przez Wykonawcę, sprzeczne z warunkami niniejszej umowy albo nakładające na Zamawiającego większe obowiązki niż wynikające z umowy nie wiążą Zamawiającego.
4. Wszelkie konieczne gwarancje należy wydać Zamawiającemu w języku polskim.

§ 8
Wynagrodzenie Wykonawcy

1. Całkowite wynagrodzenie Wykonawcy za wykonanie Przedmiotu Umowy wynosi brutto ..... zł (słownie: .....).
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszelkie koszty, jakie Wykonawca poniesie przy realizacji niniejszej umowy (np.: koszty transportu, koszty opakowania, opłaty, podatki, cła, pozostałe składniki cenotwórcze).

§ 9
Cesja

Zamawiający nie wyraża zgody na dokonanie przeniesienia w jakiejkolwiek formie i pod jakimkolwiek tytułem praw, obowiązków lub wierzytelności wynikających z realizacji umowy na rzecz osób trzecich.

§ 10
Płatność

1. Wynagrodzenie za całość dostarczonego oprogramowania będzie płatne jednorazowo na podstawie dwóch odrębnych faktur jedna faktura zgodnie z przedmiotem zamówienia określony w § 2 ust. 1 pkt 1 w ramach projektu pn. „Rozwój elektronicznych usług świadczonych przez Urząd Miasta Gorzowa Wlkp. oraz udostępniania danych publicznych" (klasyfikacje budżetowe: 750/75095/6057, 750/75095/6059) na kwotę brutto ..... (słownie: .....).

Druga faktura za przedmiot zamówienia określony w § 2 ust. 1 pkt 2 w ramach zadania „Wydatki i zakupy inwestycyjne związane z informatyką na potrzeby Urzędu Miasta" (klasyfikacja budżetowa: 750/75023/6050) na kwotę brutto .....(słownie: .....), wystawionych zgodnie z obowiązującymi przepisami, na konto bankowe wskazane na fakturach, w terminie 21 dni od daty wpływu prawidłowo wystawionych faktur do Urzędu Miasta. Na fakturach należy umieścić zapis „Termin płatności zgodnie z umową". Podstawą wystawienia faktur jest Protokół Odbioru jakościowo – ilościowego dostarczonego przedmiotu zamówienia, bez uwag.

3. Zamawiający ma prawo wstrzymać zapłatę za dostawę, jeżeli sprzęt i oprogramowanie zostanie dostarczone niezgodnie z umową, w stanie uszkodzonym lub z wadami – do czasu wymiany na oprogramowanie pozbawione uszkodzeń lub innych wad.
4. Faktury mają być wystawione i dostarczone na adres płatnika: Miasto Gorzów Wlkp. - Urząd Miasta Gorzowa Wlkp. ul. Sikorskiego 3-4, 66-400 Gorzów Wlkp. NIP 599-00-19-632.
5. Zamawiający upoważnia niniejszym Wykonawcę do wystawienia faktur bez podpisu Zamawiającego.

§ 11
Zmiany w umowie

1. Zmiany postanowień zawartej umowy mogą być dokonywane:
   1) w zakresie aktualizacji danych Wykonawcy,
   2) w przypadku zmiany obowiązujących przepisów prawa, odnoszących się do niniejszej umowy,
   3) w przypadku wystąpienia wszelkich obiektywnych zmian, niezbędnych do prawidłowego wykonania przedmiotu umowy, jeżeli taka zmiana leży w interesie publicznym,
   4) wycofania z rynku lub zaprzestania produkcji zaoferowanego przez Wykonawcę sprzętu i oprogramowania. W takiej sytuacji Zamawiający może wyrazić zgodę na zamianę sprzętu i oprogramowania będącego przedmiotem umowy na inny, o lepszych bądź takich samych cechach, parametrach i funkcjonalności pod warunkiem otrzymania oświadczenia producenta o zaprzestaniu produkcji i uzyskaniu akceptacji propozycji zmiany. Zmiana sprzętu i oprogramowania nie może spowodować zmiany ceny, terminu wykonania, okresu gwarancji oraz innych warunków realizacji umowy,
   5) w przypadku wystąpienia siły wyższej, np.: wystąpienia zdarzenia losowego wywołanego przez czynniki zewnętrzne, którego nie można było przewidzieć z pewnością, w szczególności zagrażającego bezpośrednio życiu lub zdrowiu ludzi lub grożącego powstaniem szkody w znacznych rozmiarach.

§ 12
Rozwiązanie umowy

Zamawiający ma prawo rozwiązać umowę bez zachowania okresu wypowiedzenia w każdym czasie, jeżeli Wykonawca nie wywiązuje się właściwie z zobowiązań ciążących na nim z mocy postanowień niniejszej umowy, po uprzednim pisemnym wezwaniu Wykonawcy do zaprzestania naruszeń umowy oraz usunięcia skutków naruszeń uprzednio

zaistniałych i bezskutecznym upływie jednostronnie wyznaczonego odpowiedniego terminu ich usunięcia.

§ 13
Odstąpienie od umowy

1. Zamawiający zastrzega sobie prawo do odstąpienia od całości lub części niezrealizowanej umowy, w przypadku nienależytego wykonania umowy ze skutkiem natychmiastowym w następujących przypadkach:
   1) niedostarczenia sprzętu i oprogramowania w terminie wskazanym w § 3,
   2) ujawnienia sprzętu i oprogramowania niebędącego fabrycznie nowym w terminie określonym w § 6 ust. 2,
   3) ujawnienia w dostarczonym sprzęcie i oprogramowaniu wad fizycznych lub prawnych w terminie określonym w § 6 ust. 2,
   4) innego rodzaju nienależytego wykonania lub niewykonania umowy, czyniącego dalsze jej realizowanie bezprzedmiotowym
   5) wraz z bezskutecznym upływem terminu § 6 ust. 3,
   6) w przypadku przekroczenia kwoty kar określonych w § 14 ust. 4.
2. Zamawiający może odstąpić od umowy w przypadku zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
3. W przypadku, o którym mowa w ust. 2, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

§ 14
Kary umowne

1. Zamawiającemu przysługiwać będzie kara umowna w wysokości 10% wartości umowy brutto, określonej w § 8 ust. 1 w razie odstąpienia przez Wykonawcę od realizacji umowy z przyczyn leżących po stronie Wykonawcy.
2. W przypadku odstąpienia od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy Zamawiającemu będzie przysługiwać kara umowna w wysokości 10% wartości umowy brutto, określonej w § 8 ust. 1.
3. Zamawiający zastrzega możliwość naliczenia kar umownych w wysokości 0,1 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1 - za każdy dzień opóźnienia w sytuacji, gdy Wykonawca przekroczy termin określony w § 3.
4. Wysokość kar umownych, naliczonych wg treści § 14 ust.1- 3 nie może przekroczyć 15 % wartości umowy brutto, określonej w § 8 ust. 1.
5. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych, określonych w Kodeksie Cywilnym.
6. W przypadku zaistnienia sytuacji, w których konieczne będzie naliczenie kar umownych, Zamawiający oświadcza, że wystawi Wykonawcy notę zawierającą szczegółowe naliczenie kar.
7. Kara umowna będzie potrącona z wynagrodzenia należnego Wykonawcy. W przypadku braku możliwości potrącenie kar z wynagrodzenia – termin zapłaty przez Wykonawcę z tytułu kar umownych ustala się na 14 dni od daty przekazania Wykonawcy noty księgowej.

§ 15
Poufność

Strony ustalają, iż wszystkie informacje dotyczące umowy, jak również informacje o Zamawiającym i jego działalności, o których Wykonawca dowiedział się przy realizacji umowy będą traktowane jako poufne i nie będą udostępniane osobom trzecim zarówno ustnie, jak i pisemnie lub w jakikolwiek inny sposób, z zastrzeżeniem przypadków przewidzianych przepisami prawa.

§ 16
Inne postanowienia umowy

1. Wszelkie zmiany wymagają formy pisemnej - aneksu do umowy pod rygorem ich nieważności.
2. Forma pisemna obowiązuje również przy składaniu wszelkich oświadczeń i zawiadomień oraz przesyłaniu korespondencji.
3. Strony poinformują się wzajemnie o zmianie adresu lub siedziby. W przeciwnym razie pisma dostarczone pod adres wskazany w niniejszej umowie uważane będą za doręczone.
4. Strony uzgadniają, że osobami uprawnionymi do uzgodnień i koordynacji związanych z wykonaniem niniejszej umowy są:
   Ze strony Zamawiającego:
   1) Imię i nazwisko: Andrzej Kuźba
   tel.: (95) 735 56 06, e-mail: andrzej.kuzba@um.gorzow.pl
   2) Ze strony Wykonawcy:
   Imię i nazwisko:
   tel....., email: .....
5. Zmiany osób wskazanych do uzgodnień i koordynacji, adresów korespondencyjnych, telefonów, Strony mogą dokonywać na podstawie pisemnego powiadomienia z 7-dniowym wyprzedzeniem.
6. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy Kodeksu Cywilnego oraz przepisy innych ustaw.
7. Ewentualne spory rozpatrywać będzie właściwy Sąd Powszechny właściwy dla siedziby Zamawiającego.

- Integralną część niniejszej Umowy stanowią następujące załączniki:
  1) Załącznik nr 1 - Opis Przedmiotu Zamówienia
  2) Załącznik nr 2 - Formularz Ofertowy Wykonawcy
  3) Załącznik nr 3 - Protokół Odbioru (wzór)

8. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach – po jednym egzemplarzu dla każdej ze stron.
9. Umowa wchodzi w życie z dniem podpisania.

ZAMAWIAJĄCY: WYKONAWCA:

....

DYREKTOR Wydziału Zarządzania Systemami Informatycznymi Andrzej Kuźba

ADWOKAT Zygmunt Hordyński

Załącznik nr 1

Załącznik do umowy Nr .....
Szczegółowy Opis Przedmiotu Zamówienia

1. Platforma serwerowa oraz infrastruktura dla Hurtowni danych

W ramach realizacji zamówienia Wykonawca dostarczy, skonfiguruje, wdroży i uruchomi do pełnej funkcjonalności środowisko 6 serwerów fizycznych wraz z 4 macierzami dyskowymi oraz sprzętem serwerowym przeznaczonych do montażu w szafie RACK. Dostarczony powyższy sprzęt powinien zawierać systemy operacyjne oraz oprogramowanie serwerowe niezbędne do uruchomienia w pełni działającego i funkcjonalnego środowiska serwerowego współpracującego z innym sprzętem dostarczonym przez Wykonawcę oraz ze sprzętem komputerowym posiadanym przez Zamawiającego.

Przy każdym produkcie należy podać cenę jednostkową produktu brutto i łączną cenę produktu brutto.

Dostarczane środowisko serwerów musi zostać skonfigurowane w następujący sposób:

- Serwery mają mieć możliwość uruchamiania się zarówno z macierzy i z zainstalowanych w serwerach dyskach. Wykonawca w trakcie wdrożenia wybierze jeden z wariantów.
- Sześć fizycznych serwerów będą tworzyły środowisko wirtualizacyjne, na których zainstalowane zostaną wirtualne maszyny hostujące inne serwisy funkcjonujące w systemie. Na każdy z serwerów fizycznych będą przypadać co najmniej dwa serwery wirtualne. Niniejsze serwery będą przeznaczone między innymi jako serwery aplikacji i terminali.
- Wykonawca dostarczy niezbędną ilość systemów operacyjnych do poprawnej pracy wskazanej liczby urządzeń obejmujące wszystkie dostarczane procesory.
- W ramach dostawy Wykonawca zainstaluje i skonfiguruje środowisko wirtualizacyjne. Konfiguracja platformy ma umożliwić pracę z wysoką niezawodnością (automatyczne przenoszenie maszyn wirtualnych z uszkodzonej maszyny fizycznej) oraz możliwość przenoszenia maszyn wirtualnych pomiędzy maszynami fizycznymi bez przerywania ich pracy. Wykonawca dostarczy narzędzia umożliwiające centralne zarządzanie całym środowiskiem oraz aktualizację środowiska.
- Dostarczone serwery zostaną połączone z dostarczonymi macierzami dyskowymi minimum 2 połączeniami, tak aby był zapewniona funkcja Wysokiej Dostępności - HA.
- Oferowane rozwiązanie musi być odporne na pojedynczy punkt awarii serwerów, a w szczególności awarię zasilacza, poszczególnych kart sieciowych w serwerach, wentylatorów.
- Wykonawca dostarczy komplet urządzeń i kabli przyłączeniowych do połączenia serwerów do dostarczanej infrastruktury sieciowej oraz macierzy dyskowych.
- Wykonawca dostarczy, zainstaluje i skonfiguruje sprzęt w ilościach:
    - Zestaw sześciu serwerów rack z obudową przeznaczoną do montażu w szafie RACK – 1 komplet;
    - Zestaw czterech macierzy dyskowych wraz oprogramowaniem do backupu danych – 1 komplet;
    - Systemy operacyjne na każdy z serwerów – 1 komplet;

System usług katalogowych

Wykonawca dostarczy, zainstaluje, skonfiguruje i dostosuje do potrzeb Zamawiającego system usług katalogowych wspierający funkcjonowanie pozostałych systemów informatycznych eksploatowanych przez Zamawiającego.

System usług katalogowych musi zapewnić następującą funkcjonalność:

- Odzwierciedlenie struktury organizacyjnej Zamawiającego,
- Zcentralizowane zarządzanie kontami użytkowników i ich prawami dostępu do zasobów,
- Zcentralizowane zarządzanie zasadami grup,
- Delegacja uprawnień administracyjnych,
- Możliwość implementacji mechanizmów silnego uwierzytelniania użytkowników w oparciu o karty chipowe,
- Ruch synchronizacyjny systemu usług katalogowych musi być ograniczony do minimum,
- W ramach systemu usług katalogowych uruchomione zostaną następujące usługi sieciowe:
  - DNS – hierarchiczny system rozwiązywania nazw sieciowych,
  - WINS – system rozwiązywania nazw sieciowych,
  - DHCP- system automatycznej dystrybucji ustawień sieciowych,
- System automatycznej dystrybucji poprawek i aktualizacji systemowych.

System kopii zapasowych

Wykonawca dostarczy, zainstaluje, skonfiguruje i dostosuje do potrzeb Zamawiającego system kopii zapasowych wspierający funkcjonowanie pozostałych systemów informatycznych eksploatowanych przez Zamawiającego.

System kopii zapasowych musi zapewnić następującą funkcjonalność:

- System kopii zapasowych danych produkcyjnych będzie realizowany bezagentowo bez konieczności przerywania pracy,
- Rozwiązanie ma zapewnić wysoką wydajność, wysoką dostępność usług i łatwą skalowalność stosownie do zwiększających się potrzeb,
- System backupu ma zawierać scentralizowaną konsolę backupu, w której zostaną skonfigurowane procesy backupu serwerów, baz danych i aplikacji, wraz z systemem powiadomień uwzględniających stan wykonanych kopii.

Wdrożenie

- Całość prac powinna przebiegać w sposób płynny i jak najmniej inwazyjny. Oznacza to, iż nowa konfiguracja powinna zostać przygotowana i zweryfikowana przed rozpoczęciem wdrożenia. Proces konfiguracji powinien odbyć się w siedzibie Wykonawcy i obejmować swoim zakresem tematy wcześniej ustalone ze Zleceniodawcą.
- Formą akceptacji wszystkich prac będzie protokół odbioru, który będzie podpisywany pomiędzy Kierownikiem Projektu ze strony Wykonawcy i upoważnionym przedstawicielem Zamawiającego.
- Zamawiający dokona weryfikacji przekazanych protokołem odbioru wyników prac w terminie 7 dni roboczych od daty przekazania prac.

- W przypadku stwierdzenia przez Zamawiającego zastrzeżeń, wad, uwag bądź rozbieżności pomiędzy przekazanymi do weryfikacji wynikami danego etapu, a założeniami przyjętymi dla wykonania przedmiotu Umowy, Zamawiający sporządzi i przekaże Wykonawcy w terminie 7 dni roboczych od daty przekazania prac protokół rozbieżności.
- Po otrzymaniu protokołu rozbieżności, Wykonawca w terminie 4 dni roboczych lub innym wzajemnie uzgodnionym terminie dokona koniecznych poprawek, zmian lub udzieli wiążących wyjaśnień w tej sprawie i przekaże wyniki danego etapu do ponownej weryfikacji.
- Odbiór wykonanych prac uważa się za zakończony z chwilą podpisania bez zastrzeżeń odpowiedniego protokołu odbioru przez obie Strony, w ilości po jednym egzemplarzu dla każdej ze Stron
- Wykonawca ma zapewnić kierownika projektu.
- Wykonawca ma zapewnić pracowników do realizacji projektu z kompetencjami potwierdzonymi certyfikatami producenta sprzętu serwerowego, macierzy i oprogramowania do backupu.

Szkolenie personelu z zakresu dostarczonego przedmiotu Zamówienia

- Szkolenia zostaną przeprowadzone dla min. 2 osób z działu IT Zamawiającego,
- Szkolenia muszą być prowadzone w sposób niekolidujący z działalnością Zamawiającego, ale jednocześnie z poszanowaniem harmonogramu czasu pracy pracowników.
- Szkolenia zostaną potwierdzone odpowiednim protokołem podpisanym przez obydwie strony,
- Wykonawca, uzgodni z Zamawiającym szczegółowy harmonogram szkoleń,
- Szkolenia odbędą się w autoryzowanym ośrodku szkoleniowym producenta oprogramowania,
- Szczegółowość i poziom szkoleń Wykonawca musi dobrać tak, aby przeszkolony zespół osób był w stanie samodzielnie obsługiwać i administrować dostarczonym sprzętem i oprogramowaniem,
- Zakres szkoleń musi obejmować co najmniej następujące tematy:
  - Administracja macierzami dyskowymi,
  - Administracja serwerowym systemem operacyjnym,
  - Administracja systemem wykorzystywanym do zarządzania serwerowymi systemami operacyjnymi,
  - Administracja systemem kopii zapasowych

Inne

- Wykonawca zobowiązany jest do udokumentowania zmian przeprowadzonych w systemie informatycznym Zamawiającego w dokumentacji powdrożeniowej. Dokumentacja ta powinna obejmować wszelkie dokonane zmiany, opisywać proces wdrożenia i działanie nowego oprogramowania i urządzeń wraz z procedurami konfiguracji zadań backupowych i przywracania kopii zapasowych zarówno do środowiska produkcyjnego jak i testowego. Wszelkie materiały muszą być w języku polskim.
- Wykonawca zobowiązany jest przekazać Zamawiającemu pełny dostęp do wdrożonego oprogramowania wraz z wszystkimi loginami i hasłami.
- Od Wykonawcy wymaga się oddelegowania do prac wdrożeniowych personelu posiadającego certyfikaty potwierdzające kompetencje związane z oferowanymi rozwiązaniami.
- Wykonawca zobowiązany jest to zapewnienia gwarancji na wdrożoną konfigurację i przeprowadzenia

niezbędnych aktualizacji oprogramowania, przez okres minimum 3 miesięcy, po zamknięciu wdrożenia.

1.1 Serwery

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne serwerów
1	2	3
Serwery		
1.	**Typ**	Serwery
2.	**Obudowa**	-Typu Rack, wysokość maksymalnie 3U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack
3.	**Płyta główna**	-Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów dwunastordzeniowych; -Możliwość instalacji minimum 7 złącz PCI Express (3 nisko profilowych, 3 pełno profilowych) za pomocą tzw. riser-cards lub zintegrowanych w płycie głównej. -Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych)
4.	**Procesory**	-Zainstalowane dwa procesory serwerowe działające architekturze x86 (64-bit). Procesory muszą osiągać w teście SPECint_rate2006 Baseline wynik minimum 1630 pkt. w konfiguracji dwuprocesorowej. Wyniki testu muszą być opublikowane i powszechnie dostępne na stronie www.spec.org. Każdy z procesorów musi posiadać minimum 38MB pamięci Cache
5.	**Pamięć RAM**	-Zainstalowane 768 GB pamięci RAM typu DDR4 Registered o szybkości 2133MHz lub lepszej -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC lub jej odpowiednik -24 gniazda pamięci RAM na płycie głównej
6.	**Dyski twarde**	- Minimum 6 wnęk dla dysków twardych Hotplug 2,5 z przodu obudowy; - Minimum 9 wnęk dla dysków twardych Hotplug 3,5 z przodu obudowy; Dopuszczalna jest realizacja poprzez dodatkową półkę dyskową SAS 12G podpiętą do serwera. Wraz z serwerem muszą być dostarczone odpowiednie kable oraz ekspander SAS w slocie PCI-E. -Musi istnieć możliwość rozbudowy o dodatkowe 2 wnęki 2,5" z tylu lub przodu obudowy
7.	**Nośniki dostarczone wraz z serwerem**	-Dwa dyski SSD o wielkości minimum 200GB
8.	**Kontrolery LAN**	- 4 porty 10GE Ethernet na wkładki SFP+ z wkładkami typu SFP+ SR
9.	**Kontrolery I/O**	- 2 porty Fibre Channel 8Gbps z wkładkami SWL
10.	**Porty**	-zintegrowana karta graficzna -1x USB wewnętrzne – w środku obudowy -2x USB zewnętrzne typu USB 3.0 -1x złącze Display Port lub VGA
11.	**Zasilanie**	-Zainstalowane dwa redundantne zasilacze hot-plug klasy minimum 80 PLUS Titanium o mocy minimalnej 750W;
12.	**Zarządzanie out of band**	-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę WWW (http/https) oraz SSH • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Monitoring pracy wentylatorów i ich prędkości obrotowej • Synchronizacja czasu poprzez protokół NTP • Wyświetlanie informacji o komponentach zainstalowanych w serwerze (karty PCI, pamięci procesory, zasilacze) • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM). • Możliwość zdalnego wyłączenia/włączenia serwera • Możliwość zdefiniowania wielu kont administratorów oraz integracja z Active Directory lub LDAP • Karta zarządzająca musi wspierać monitoring karty RAID (logiczne volumeny, fizyczne dyski, grupy RAID) jeśli takowa jest zainstalowana w serwerze.

		• Jeśli wymagane są licencje dla wyżej opisanych funkcjonalności – należy je dostarczyć wraz z serwerem
13.	**Wspierane OS**	- Microsoft Hyper-V 2012, który posiada Zamawiający lub nowszy do którego zamawiający chce wykonać aktualizację.
14.	**Gwarancja i wsparcie**	Serwer musi posiadać pakiet serwisowy oferujący następujące warunki gwarancji: - Gwarancja 60 miesięcy na części i robociznę realizowana w miejscu eksploatacji sprzętu - Gwarancja z czasem wymiany typu następny dzień roboczy od zgłoszenia w miejscu instalacji
15.	**Termin realizacji zamówienia**	Oferowane serwery muszą być dostarczone w terminie nie dłuższym niż 6 tygodni od daty podpisania Umowy

1.2 Macierz typ I

Wszystkie opisane parametry wymagane są wymaganiami minimalnymi. Wymagania opcjonalne będą dodatkowo punktowane.

Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne serwerów**
1	**2**	**3**
Macierz typ I		
1.	**Typ**	Macierz typ I
2.	Typ Obudowy	Do instalacji w standardowej szafie rack 19". Wysokość macierzy oraz półek dyskowych nie może być większa niż 4U o gęstości min 12 dysków na każde 2U
3.	Wymagana przestrzeń dyskowa	Macierz musi być wyposażona w minimum: • 4 dyski 2,5" 400GB Flash • 12 dysków 900GB 2,5" SAS 10k rpm, • 12 dysków 4TB 3,5" NL SAS 7.2k rpm
4.	Architektura	Pojedyncza macierz złożona z co najmniej 2 kontrolerów dyskowych obsługujących ruch blokowy wymienialne bez przerywania pracy. Kontrolery pracują jednocześnie w trybie active-active. Macierz musi posiadać co najmniej 1 port do zarządzania w każdym z kontrolerów. Macierz musi obsługiwać połączenia do półek dyskowych oraz do dysków w standardzie SAS 12 Gb/s Macierz musi umożliwiać jednoczesne stosowanie półek dyskowych obsługujących dyski 2,5" oraz 3,5". Półki dyskowe 2,5" muszą umożliwiać instalację co najmniej 24 napędów dyskowych 2,5". Półki dyskowe 3,5" muszą umożliwiać instalację co najmniej 12 napędów dyskowych 3,5". Macierz powinna wpierać zasilanie z dwóch niezależnych źródeł prądu.
5.	Obsługa dysków	Macierz musi obsługiwać dyski 2,5" i 3,5" we właściwych obudowach. Macierz musi zapewniać możliwość używania różnych dysków tego samego typu – odpowiednio 2,5" i 3,5". Macierz musi obsługiwać dyski SSD, SAS oraz NL-SAS w standardzie SAS 12 Gb/s. Macierz musi obsługiwać co najmniej 248 dyski. Dyski Flash SSD muszą mieć parametr trwałości (ang. Endurance) na poziomie nie mniejszym niż 0.5 DWPD (Gdzie 1 = DWPD oznacza pełne nadpisanie całego dysku w ciągu 24 godzin co dziennie przez 5 lat)
6.	Pamięć podręczna	Pamięć podręczna każdego z kontrolerów musi być nie mniejsza niż 6 GB (sumarycznie 12 GB na macierz wyposażoną w dwa kontrolery) Pojemność pamięci cache nie może być

		osiągnięta poprzez wykorzystanie przestrzeni na dyskach SSD lub dodatkowych kartach z pamięcią flash.
7.	Porty zewnętrzne	Macierz musi być wyposażona w co najmniej 4 porty 16 Gbit FC
8.	Ochrona danych	Macierz musi obsługiwać poziomy RAID 0,1,5,6,10. Macierz powinna umożliwiać stworzenie grup RAID w których zamiast wykorzystania dysku hot spare będzie występować tzw. przestrzeń zapasowa rozłożona na wszystkich dyskach w ramach danej grupy RAID (distributed spare).
9.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami) z wykorzystaniem protokołów komunikacji takich jak: Fibre Channel, iSCSI.
10.	Ochrona spójności danych	Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. Musi istnieć funkcjonalność Cache dla procesu odczytu. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu. Musi istnieć możliwość wyłączenia cache dla poszczególnych wolumenów
11.	Mechanizmy Thin Provisioning	Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
12.	Zarządzanie grupami dyskowymi i dyskami logicznymi	Macierz musi mieć możliwość rozłożenia wolumenu logicznego pomiędzy co najmniej dwoma grupami RAID. Macierz musi obsługiwać funkcjonalności LUN Masking i LUN mapping. Macierz musi umożliwiać automatyczne równoważenie obciążenia w ramach grupy/puli dysków tego samego typu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji. Macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji.
13.	Możliwość migracji danych	Macierz musi posiadać funkcjonalność migracji danych z innych macierzy dyskowych. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
14.	Wewnętrzne kopie danych	Macierz musi mieć możliwość wykonania kopii danych typu Point-In-Time (PiT) wolumenów. Zasoby źródłowe oraz docelowe kopii PiT mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, NL-SAS). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji. Kopie danych typu PIT muszą być tworzone w trybach min. kopii pełnej (klon) oraz incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii).
15.	Zdalna replikacja danych	Macierz musi umożliwiać rozbudowę o funkcjonalność minimum replikacji asynchronicznej wolumenów logicznych pomiędzy dwoma takimi samymi modelami macierzy dyskowej oraz innymi macierzami dostępnymi w ramach tej samej rodziny modelowej. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SSD, SAS, NL-SAS). Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji.
16.	Automatyczna relokacja	Macierz musi mieć możliwość rozbudowy o funkcjonalność optymalizacji wykorzystania dysków SSD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów

	danych	wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migrację na dyski SSD. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD i automatycznie migrować z dysków SSD nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD, Enterprise (15k i 10K) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu.
17.	Administracja	Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie musi być dostępne poprzez interfejs GUI (WWW) oraz interfejs linii poleceń (Command Line Interface). Dostęp do linii poleceń poprzez połączenie szyfrowane. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie Macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI
18.	Obsługa wielu ścieżek	Macierz musi obsługiwać wiele kanałów I/O (Multipathing). Musi być zapewnione automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Musi być zapewnione przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz. Wymagana jest również obsługa równoważenia obciążenia (load balancing) pomiędzy kanałami macierzy. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania.
19.	Wsparcie serwisowe	5-letnia gwarancja producenta w miejscu instalacji, z czasem reakcji NBD (następny dzień roboczy) okno zgłoszeniowe 24/7 świadczona przez polski oddział serwisowy producenta macierzy. Wszystkie dyski uszkodzone w okresie trwania wsparcia serwisowego nie wymagają zwrotu po wymianie na sprawne - DMR (Defective Media Retention). W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.
20.	Usługi	Usługi instalacji i konfiguracji funkcjonalności oprogramowania macierzy dostarczonych wraz z macierzą.

21.	Dodatkowe wymagania	Macierz musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie RP. Macierz powinna umożliwiać migrację do wyższych modeli macierzy w ramach tej samej rodziny modelowej poprzez wymianę kontrolerów. Macierz musi posiadać funkcjonalność zarówno zwiększania jak i zmniejszania rozmiaru wolumenów. Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia wykonywanych na danym wolumenie. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego wolumenu. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy. Kopie danych typu PIT muszą być tworzone w trybach kopii pełnej (klon) oraz kopii wskaźników (migawka), incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii), multitarget (wiele kopii z jednego źródła), cascaded (kopia z kopii). Macierz powinna umożliwiać rozbudowę o funkcjonalność replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy dwoma takimi samymi modelami macierzy dyskowej oraz innymi macierzami dostępnymi w ramach tej samej rodziny modelowej. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SSD, SAS, NL-SAS). Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji.

1.3 Macierz typ II

Wszystkie opisane parametry wymagane są wymaganiami minimalnymi. Wymagania opcjonalne będą dodatkowo punktowane.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne serwerów
1	2	3
Macierz typ II		
1.	**Typ**	Macierz typ II
2.	Typ Obudowy	Do instalacji w standardowej szafie rack 19". Wysokość macierzy oraz półek dyskowych nie może być większa niż 4U o gęstości min. 12 dysków na każde 2U Macierz musi umożliwiać zastosowanie półek dyskowych wysokiej gęstości (co najmniej 24 dyski na 2U wysokości).
3.	Wymagana przestrzeń dyskowa	Macierz musi być wyposażona w minimum: • 18 dysków 2,5" 1.8 TB Flash Drive
4.	Architektura	Pojedyncza macierz złożona z co najmniej 2 kontrolerów dyskowych obsługujących ruch blokowy wymienialne bez przerywania pracy. Kontrolery pracują jednocześnie w trybie active-active. Macierz musi posiadać co najmniej 1 port do zarządzania w każdym z kontrolerów. Macierz musi obsługiwać połączenia do półek dyskowych oraz do dysków w standardzie SAS 12 Gb/s Wszelkie połączenia SAS pomiędzy elementami składowymi macierzy muszą być redundantne. Macierz musi wykorzystywać połączenia punkt-punkt do dysków twardych. Macierz musi cechować brak pojedynczego punktu awarii. Macierz musi umożliwiać jednoczesne stosowanie półek dyskowych obsługujących dyski

		2,5" oraz 3,5". Półki dyskowe 2,5" muszą umożliwiać instalację co najmniej 24 napędów dyskowych 2,5". Półki dyskowe 3,5" muszą umożliwiać instalację co najmniej 12 napędów dyskowych 3,5". Macierz powinna wpierać zasilanie z dwóch niezależnych źródeł prądu. Macierz powinna być odporna na zaniki napięcia , tzn chwilowy zanik napięcia nie powinien przerywać pracy macierzy. Rozbudowa o dodatkowe półki dyskowe powinna być realizowana za pomocą redundantnych połączeń SAS 12Gb. Macierz musi posiadać możliwość liniowej skalowalności parametrów wydajnościowych, zasobów dyskowych oraz ilości obsługiwanych dysków (do co najmniej 1056) poprzez dodanie kolejnych macierzy tego samego typu (co najmniej 4), przy zachowaniu jednolitego i wspólnego zarządzania zasobami dyskowymi.
5.	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS oraz NearLine-SAS 2,5" oraz 3,5" w standardach SAS 12 Gb/s i 6 Gb/s, dwuportowe, hot-swap Macierz musi obsługiwać co najmniej 248 dysków wewnętrznych. Dyski Flash SSD muszą mieć parametr trwałości (ang. Endurance) na poziomie nie mniejszym niż 0.5 DWPD (Gdzie 1 = DWPD oznacza pełne nadpisanie całego dysku w ciągu 24 godzin co dziennie przez 5 lat)
6.	Pamięć podręczna	Macierz musi być wyposażona w minimum 32GB pamięci cache ramach pary kontrolerów.
7.	Porty zewnętrzne	Musi być wyposażona w co najmniej port 16Gb FC
8.	Ochrona danych	Macierz musi obsługiwać poziomy RAID 0,1,5,6,10. Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczej półki dyskowej.
9.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami) z wykorzystaniem protokołów komunikacji takich jak: Fibre Channel, iSCSI.
10.	Ochrona spójności danych	Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. Musi istnieć możliwość wyłączenia cache dla poszczególnych wolumenów Macierz musi posiadać funkcjonalność Cache dla procesu odczytu oraz funkcjonalność Mirrored Cache dla procesu zapisu. Funkcjonalność partycjonowania pamięci cache.
11.	Mechanizmy Thin Provisioning	Macierz musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy.
12.	Zarządzanie grupami dyskowymi i dyskami logicznymi	Macierz musi mieć możliwość rozłożenia wolumenu logicznego pomiędzy co najmniej dwoma różnymi typami macierzy dyskowych. Macierz musi obsługiwać funkcjonalności LUN Masking i LUN mapping. Macierz musi umożliwiać automatyczne równoważenie obciążenia w ramach grupy/puli dysków tego samego typu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji. Macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji. Macierz musi posiadać funkcjonalność minimum zwiększania rozmiaru wolumenów. Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia

		wykonywanych na danym wolumenie. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego wolumenu. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy. Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej zbudowanej w oparciu o jedną macierz musi wynosić co najmniej 2048. Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami. Macierz musi posiadać funkcjonalność tworzenia mirrorowanych LUN, rozłożonych pomiędzy różnymi zarządzanymi zasobami dyskowymi, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować, dla maksymalnej pojemności macierzy i maksymalnej liczby wolumenów. Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych macierzach dyskowych, w szczególności pochodzących od HP, IBM, Oracle, Fujitsu, EMC i HDS. Jeżeli funkcjonalność ta wymaga licencji należy takową zaoferować odpowiednio do konfiguracji.
13.	Możliwość migracji danych	Macierz musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych, oraz wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (FC, SAS, SSD, NL-SAS/SATA). Macierz musi posiadać funkcjonalność migracji danych z innych macierzy dyskowych.
14.	Wewnętrzne kopie danych	Macierz musi mieć możliwość wykonania kopii danych typu Point-In-Time (PiT) wolumenów. Zasoby źródłowe oraz docelowe kopii PiT mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (FC, SSD, SAS, NL-SAS/SATA), jak również na odrębnych, zwirtualizowanych poprzez przedmiotową macierz podsystemach dyskowych. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji. Kopie danych typu PIT muszą być tworzone w trybach kopii pełnej (klon) oraz kopii wskaźników (migawka), incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii), multitarget (wiele kopii z jednego źródła), cascaded (kopia z kopii). Macierz musi obsługiwać min. 255 kopii migawkowych per wolumen.
15.	Zdalna replikacja danych	Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy dwoma takimi samymi modelami macierzy oraz innymi modelami macierzy dostępnymi w ramach jednej rodziny modelowej danego producenta. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (FC, SAS, SSD, NL-SAS/SATA) w szczególności na różnych, zwirtualizowanych przez macierz systemach dyskowych. Replikacja musi być realizowana zarówno przy użyciu interfejsów Fibre Channel jak i protokołu IP. Przy replikacji z wykorzystaniem protokołu IP kontrolery macierzy musza zapewniać mechanizm optymalizacji transmisji danych po IP. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji.
16.	Automatyczna relokacja danych	Macierz musi optymalizować wykorzystanie dysków SSD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych (wewnętrznych jak i zewnętrznych - zwirtualizowanych) oraz ich automatyczną migrację na dyski SSD. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD i automatycznie migrować z dysków SSD nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD, Enterprise (15k i 10K) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji.

17.	Kompresja danych	Wsparcie dla kompresji danych w trybie inline („na bieżąco") bez potrzeby zapisywania danych na nośnikach danych w formie nieskompresowanej) dla dostępu blokowego. Kompresja musi być realizowana poprzez dedykowane zasoby sprzętowe przeznaczone do tego celu. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.
18.	Administracja	Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie musi być dostępne poprzez interfejs GUI (WWW) oraz interfejs linii poleceń (Command Line Interface). Dostęp do linii poleceń poprzez połączenie szyfrowane. Macierz powinna umożliwiać tworzenie skryptów użytkownika. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie Macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI
19.	Obsługa wielu ścieżek	Macierz musi obsługiwać wiele kanałów I/O (Multipathing). Musi być zapewnione automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Musi być zapewnione przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz. Wymagana jest również obsługa równoważenia obciążenia (load balancing) pomiędzy kanałami macierzy. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania.
20.	Wsparcie serwisowe	5-letnia gwarancja producenta w miejscu instalacji, z czasem reakcji NBD (następny dzień roboczy) okno zgłoszeniowe 24/7 świadczona przez polski oddział serwisowy producenta macierzy. Wszystkie dyski uszkodzone w okresie trwania wsparcia serwisowego nie wymagają zwrotu po wymianie na sprawne - DMR (Defective Media Retention). W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.
21.	Usługi	Usługi instalacji i konfiguracji funkcjonalności oprogramowania macierzy dostarczonych wraz z macierzą.

22.	Dodatkowe wymagania	Macierz musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie RP. Macierz powinna umożliwiać migrację do wyższych modeli macierzy w ramach tej samej rodziny modelowej poprzez wymianę kontrolerów. Macierz musi posiadać funkcjonalność zarówno zwiększania jak i zmniejszania rozmiaru wolumenów. Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia wykonywanych na danym wolumenie. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego wolumenu. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy. Kopie danych typu PIT muszą być tworzone w trybach kopii pełnej (klon) oraz kopii wskaźników (migawka), incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii), multitarget (wiele kopii z jednego źródła), cascaded (kopia z kopii). Macierz musi umożliwiać rozbudowę o funkcjonalność replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy dwoma takimi samymi modelami macierzy dyskowej oraz innymi macierzami dostępnymi w ramach tej samej rodziny modelowej. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SSD, SAS, NL-SAS). Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji. Możliwość wirtualizacji zasobów znajdujących się na na macierzach różnych producentów w trybie natywnym tzn. takim, w którym dane w przypadku awarii wirtualizatora mogą być odczytane bez jego udziału. Nie mniej niż 8 połączeń FC do macierzy od strony hostów. Interfejsy FC muszą pracować w trybie co najmniej 8 Gb/s FC. Macierz musi zapewniać instalację dodatkowych 8 portów Fibre Channel bez konieczności wymiany kontrolerów lub instalacji dodatkowych kontrolerów. Macierz musi mieć co najmniej 6 portów iSCSI, 1Gb Eth oraz musi posiadać możliwość rozbudowy o 8 portów 10 GbE FCoE/iSCSI.

2. Oprogramowanie do wirtualizacji oraz oprogramowanie systemów serwerowych

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne oprogramowania
1	2	3
Oprogramowanie do wirtualizacji oraz oprogramowanie systemów serwerowych		
1.	**Typ**	Oprogramowanie do wirtualizacji oraz oprogramowanie systemów serwerowych
2.	**Wymagania minimalne dostarczanych licencji**	Wszystkie dostarczane licencje muszą min. spełniać wymagania: • Licencje bezterminowe muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi (np. w przypadku wymiany stacji roboczej lub serwera). • Licencje muszą pozwalać na sublicencjonowanie w ramach gminy • Wymagane jest zapewnienie możliwości korzystania z kopii zamiennych (możliwość instalacji oprogramowania na wielu urządzeniach przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych. • W ramach umowy Wykonawca ma zapewnić możliwość do pobierania kodu zamówionego oprogramowania i kluczy licencyjnych w terminie nie dłuższym niż 10 dni roboczych od podpisania umowy. • Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej

		upoważnionym osobom ze strony Zamawiającego na: - Pobieranie zakupionego oprogramowania, - Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania, - Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów. • Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym. •
3.	**Serwerowy system operacyjny**	Licencja na serwerowy system operacyjny musi być przypisana do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Oprogramowanie musi być licencjonowane na minimum 44 fizyczne rdzenie procesorów serwerów fizycznych, na których zostanie zainstalowany serwerowy system operacyjny. Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania, do 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 240 procesorów wirtualnych oraz 12TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Graficzny interfejs użytkownika. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 21. Możliwość implementacji następujących funkcjonalności: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. 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), z możliwością wykorzystania następujących funkcji: i. Podłączenie SSO do domeny usługi katalogowej w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. Powyższa funkcjonalność ma być podstawą dla stworzenia usługi katalogowej dla organizacji Zamawiającego. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), (obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 22. 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. 23. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). 24. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 25. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 26. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 27. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
4.	**Pakiet licencji dostępowych**	Pakiet licencji dostępowych do serwerowego systemu operacyjnego dla użytkowników wewnętrznych. Licencje muszą zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników wewnętrznych funkcjonalności serwerowych systemów operacyjnych.
5.	**System zarządzania środowiskami serwerowymi**	Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego rdzenia procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 44 fizyczne rdzenie procesorów serwerów zarządzanych. Licencja musi uprawniać do zarządzania dowolną liczbą środowisk systemu operacyjnego na tym serwerze. Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej

		modułach: - System zarządzania infrastrukturą i oprogramowaniem - System zarządzania komponentami - System zarządzania środowiskami wirtualnym - System tworzenia kopii zapasowych - System automatyzacji zarządzania środowisk IT - System zarządzania incydentami i problemami - Ochrona antymalware **System zarządzania infrastrukturą i oprogramowaniem** System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 1. Inwentaryzacja i zarządzanie zasobami: a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania b. 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 c. 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...) d. 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 e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera 2. Użytkowane oprogramowanie – pomiar wykorzystania a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego. 3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych. 4. Definiowanie i sprawdzanie standardu serwera: a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej, b. Reguły powinny sprawdzać następujące elementy systemy komputerowego: i. stan usługi ii. obecność poprawek (Hotfix) iii. WMI iv. rejestr systemowy v. system plików vi. Active Directory vii. SQL (query) viii. Metabase 5. Raportowanie, prezentacja danych: a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services c. System powinien posiadać predefiniowane raport w następujących kategoriach: i. Sprzęt (inwentaryzacja) ii. Oprogramowanie (inwentaryzacja) iii. Oprogramowanie (wykorzystanie) iv. Oprogramowanie (aktualizacje, w tym system operacyjny) d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu 6. Analiza działania systemu, logi, komponenty

		a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym. System zarządzania komponentami System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania: 7. Architektura a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być dostępne dla klientów systemu w celu automatycznej konfiguracji. b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług. c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych. d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny. e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych. f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany. g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN). h. Wsparcie dla protokołu IPv6. i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta. 8. Audyt zdarzeń bezpieczeństwa System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować: a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących). b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji. c. 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. 9. Konfiguracja i monitorowanie System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym: a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z: i. rejestru ii. WMI iii. OLEDB iv. LDAP v. skrypty (uruchamiane w celu wykrycia atrybutów obiektu), W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi. b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp. c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp. elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:

		i. Windows Server 2003/2008/2008R2 ii. Active Directory 2003/2008 iii. Exchange 2003/2007/2010 iv. Microsoft SharePoint 2003/2007/2010 v. Microsoft SharePoint Services 3.0 vi. Microsoft SharePoint Foundation 2010 vii. SQL 2005/2008/2008R2 (x86/x64/ia64) viii. Windows Client OS (XP/Vista/7) ix. Information Worker (Office, IExplorer, Outlook, itp.) x. IIS 6.0/7.0/7.5 xi. HP-UX 11i v2/v3 xii. Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86) xiii. Red Hat Enterprise Linux 4/5/6 (x86/x64) Server xiv. Novell SUSE Linux Enterprise Server 9/10SP1/11 xv. IBM AIX v5.3 i v6.1/v7.1 (POWER) d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego. e. 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: i. interfejsy sieciowe ii. porty iii. sieci wirtualne (VLAN) iv. grupy Hot Standby Router Protocol (HSRP) f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych: i. SNMP (trap, probe) ii. WMI Performance Counters iii. Log Files (text, text CSV) iv. Windows Events (logi systemowe) v. Windows Services vi. Windows Performance Counters (perflib) vii. WMI Events viii. Scripts (wyniki skryptów, np.: WSH, JSH) ix. Unix/Linux Service x. Unix/Linux Log g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów 10. Tworzenie reguł a. w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych: i. Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event) ii. Performance based (SNMP performance, WMI performance, Windows performance) iii. Probe based (scripts: event, performance) b. 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. c. 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: i. na ilość takich samych próbek o takiej samej wartości ii. na procentową zmianę od ostatniej wartości próbki. d. 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 czasu. e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji. f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:

		i. ASP .Net Application ii. ASP .Net Web Service iii. OLE DB iv. TCP Port v. Web Application vi. Windows Service vii. Unix/Linux Service viii. Process Monitoring Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji. h. 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). i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych. j. 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, avg). 11. Przechowywanie i dostęp do informacji a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp.) powinny być przechowywane w bazie danych operacyjnych. b. 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 w oparciu o najświeższe dane. c. 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). d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności. e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych. f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów: i. XML ii. CSV iii. TIFF iv. PDF v. XLS vi. Web archive 12. Konsola systemu zarządzania a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli. b. System powinien udostępniać dwa rodzaje konsoli: i. w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna) ii. w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa). c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach: i. Alerts ii. Events iii. State iv. Performance v. Diagram vi. Task Status vii. Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych

		elementów systemu). d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie. e. 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". f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu. g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym: i. opcji definiowania ról użytkowników ii. opcji definiowania widoków iii. opcji definiowania i generowania raportów iv. opcji definiowania powiadomień v. opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących vi. opcji instalacji/deinstalacji klienta h. 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). 13. Wymagania dodatkowe a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na: i. Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo), ii. Wykonywanie operacji w systemie z poziomu linii poleceń, iii. Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania, iv. Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie, **System zarządzania środowiskami wirtualnym** System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy: 1. Architektura a. System zarządzania środowiskiem wirtualnym powinien składać się z: - serwera zarządzającego, - relacyjnej bazy danych przechowującej informacje o zarządzanych elementach, - konsoli, instalowanej na komputerach operatorów, - portalu self-service (konsoli webowej) dla operatorów „departamentowych", - biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych, - agenta instalowanego na zarządzanych hostach wirtualizacyjnych, - „konektora" do systemu monitorującego pracę hostów i maszyn wirtualnych. b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over). c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców. 2. Interfejs użytkownika a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny. b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów. c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp. d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit. e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań. 3. Scenariusze i zadania a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny

		wirtualnej w co najmniej dwóch trybach: • Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny, • Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych: - profilu sprzętowego - profilu systemu operacyjnego, - przygotowanych dysków twardych, b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania. c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami: • w trybie migracji „on-line" – bez przerywania pracy, • w trybie migracji „off-line – z zapisem stanu maszyny d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami. e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta. f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu. g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej. h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji. 4. Wymagania dodatkowe a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę. b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania. c. System musi kreować raporty z działania zarządzanego środowiska, w tym: • utylizacja poszczególnych hostów, • trend w utylizacji hostów, • alokacja zasobów na centra kosztów, • utylizacja poszczególnych maszyn wirtualnych, • komputery-kandydaci do wirtualizacji d. System musi umożliwiać skorzystanie z szablonów: • wirtualnych maszyn • usług oraz profili dla: • aplikacji • serwera SQL • hosta • sprzętu • systemu operacyjnego gościa e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów). f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej. g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją) **System tworzenia kopii zapasowych** System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania: 1. System musi składać się z: a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych b. agentów kopii zapasowych instalowanych na komputerach zdalnych c. konsoli zarządzającej d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach

		e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service) 2. System kopii zapasowych musi umożliwiać: a. zapis danych na puli magazynowej złożonej z dysków twardych b. zapis danych na bibliotekach taśmowych 3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej. 4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe. 5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej. 6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania. 7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii. 8. System kopii zapasowych powinien umożliwiać przywrócenie: a. danych plikowych b. danych aplikacyjnych c. stanu systemu (Systemstate) d. obrazu systemu operacyjnego (tzw. Bare Metal Restore) 9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych 10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości 11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy 12. System kopii zapasowych musi rozpoznawać aplikacje: a. ze względu na tworzone logi transakcyjne: • Microsoft Exchange Server • Microsoft Office Sharepoint Server • Microsoft SQL Server b. ze względu na zapewnienie nieprzerwalności pracy • Microsoft Virtual Server 2005 • Microsoft Hyper-V server 13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach 14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach 15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów 16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń 17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje" 18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych 19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych 20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.). 21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku 22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat 23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób. 24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30

		minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe. 25. System kopii zapasowych musi umożliwiać odtworzenie danych do: a. lokalizacji oryginalnej b. lokalizacji alternatywnej c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych **System automatyzacji zarządzania środowisk IT** System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk. 1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie. 2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT. 3. System musi wspomagać planowanie i automatyzację wdrażania poprawek. 4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych. 5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow. **System zarządzania incydentami i problemami** System zarządzania incydentami i problemami musi spełniać następujące wymagania: 1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna) 2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą. 3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami. 4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie. 5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać: a. Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką, b. Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia, c. Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu, d. Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania, e. Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów, f. Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej, g. Tworzenie baz wiedzy na temat rozwiązywania problemów, h. Automatyzację działań w przypadku znanych i opisanych problemów, i. Wykrywanie odchyleń od założonych standardów ustalonych dla systemu. **Ochrona antymalware** Oprogramowanie antymalware musi spełniać następujące wymagania: 1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day. 2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem 3. Centralne zarządzanie politykami ochrony. 4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony. 5. Mechanizmy wspomagające masową instalację. 6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy

		zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego. 7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania. 8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia. 9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.). 10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania. 11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

3. Przeszkolenie

Wykonawca dostarczy vouchery dla min. 2 administratorów IT do zrealizowania w autoryzowanym ośrodku szkoleniowym producenta oprogramowania, zgodnie z poniższymi wymaganiami minimalnymi.

Wymagania minimalne:

- Vouchery muszą być ważne przez okres co najmniej 12 miesięcy od daty podpisania Protokołu Odbioru ilościowego.
- Szkolenia muszą zostać przeprowadzone w takich sposób, aby zrealizowały każdy z wymaganych minimalnych zakresów tematycznych oraz aby po ich zakończeniu uczestnicy zostali przygotowani do zdania certyfikowanych egzaminów potwierdzających zdobyte umiejętności w certyfikowanych ośrodkach producenta oprogramowania.

Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry szkolenia**
1	2	3
Szkolenia		
1.	**Typ**	Szkolenia
2.	**Minimalny zakres tematyczny**	1. Instalację, aktualizację oraz migrację serwerowego systemu operacyjnego. 2. Zarządzanie lokalnym magazynem danych. 3. Implementowanie rozwiązań magazynowania danych typu Enterprise. 4. Instalacja, konfiguracja i zarządzanie maszynami wirtualnymi. 5. Wdrażanie i zarządzanie kontenerami. 6. Przegląd metod wysokiej dostępności i równoważenia zarządzania zasobami. 7. Implementowanie i zarządzanie zasobami typu klastrowego. 8. Zarządzanie, monitorowanie i utrzymanie instalacji maszyn wirtualnych. 9. Implementację infrastruktury sieciowej.

		10.	Implementację DHCP/DNS.
		11.	Zdalny dostęp do serwerowego systemu operacyjnego.
		12.	Implementacja dostępu VPN.
		13.	Implementacja usług sieciowych dla oddziałów.
		14.	Implementacja sieciowych rozwiązań programowych
		15.	Instalacja i konfiguracja usług domenowych.
		16.	Zarządzanie obiektami usług domenowych.
		17.	Wdrażanie i zarządzanie certyfikatami.

Projekt współfinansowany ze środków Unii Europejskiej, Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego LUBUSKIE 2020

Załącznik nr 3

Załącznik do umowy Nr .....

PROTOKÓŁ ODBIORU

Numer umowy:			
Projekt:	Rozwój elektronicznych usług świadczonych przez Urząd Miasta Gorzowa Wlkp. oraz udostępniania danych publicznych.		
Zamawiający:	Miasto Gorzów Wlkp. - Urząd Miasta Gorzowa Wlkp.		
Data odbioru:		**Miejsce:**	Gorzów Wlkp.
Nazwa Usługi / Zadania:	Dostawa wraz z wdrożeniem platformy serwerowej oraz infrastruktury dla Hurtowni Danych wraz z oprogramowaniem do wirtualizacji oraz oprogramowaniem systemów serwerowych		

Historia dokumentu. Statusy zapisów: Nowy, Zamiana, Weryfikacja.

Wersja	Data wersji	Opis	Status zapisu	Dotyczy	Autorzy	Zatwierdził:
1.00	30-05-2017	Pierwsza wersja dokumentu	NOWY			

Produkty przekazane do odbioru (Zadanie I):

Nazwa produktu:	Wersja odbierana:	Forma przekazania produktu:

Produkty przekazane do odbioru (Zadanie II):

Nazwa produktu:	Wersja odbierana:	Forma przekazania produktu:

Wykonawca (w dniu) dostarczył .....

Wykonawca (w dniu) zainstalował .....

Protokół jest / ~~nie jest~~ podstawą do wystawienia faktury.

Ze strony Zamawiającego	Ze strony Wykonawcy