**Załącznik nr 1b do SIWZ**

**Szczegółowy opis przedmiotu zamówienia dla zadania częściowego nr 2**

1. **Przedmiotem zamówienia jest dostawa oprogramowania do backupu środowiska wirtualnego VMware i rozszerzenie posiadanych przez Zamawiającego licencji na oprogramowanie do wirtualizacji wraz ze wsparciem producenta.**
   1. Zakres przedmiotu zamówienia obejmuje:
      1. dostawę 12 licencji na oprogramowanie (zwane dalej „Systemem”) do tworzenia kopii bezpieczeństwa zwirtualizowanego środowiska VMware vSphere w wersji 6.0 lub nowszej (posiadanego przez zamawiającego), dla 3 (trzech) 4-procesorowych serwerów klasy x86 (4 fizyczne procesory), bez limitu ilości maszyn wirtualnych podlegających wykonaniu kopii bezpieczeństwa. Dostarczone licencje muszą być niewyłączne   
         i bezterminowe oraz muszą umożliwiać realizację wszystkich funkcjonalności opisanych w punkcie 2.
      2. dostarczenie rozszerzenia posiadanych przez Zamawiającego licencji lub równoważnych dla oprogramowania do wirtualizacji (Zamawiający posiada licencje VMware Vsphere 6 Enterprise Plus (Per CPU) oraz oprogramowania zarządzającego VMware vCenter Server 6 Standard for vSphere 6 (Per Instance). Dostarczone licencje muszą być niewyłączne   
         i bezterminowe oraz muszą umożliwiać realizację wszystkich funkcjonalności opisanych w punkcie 10.
      3. przeprowadzenie instalacji, konfiguracji i wdrożenia dostarczonego oprogramowania do backupu środowiska wirtualnego Vmware oraz przygotowanie dokumentacji, o której mowa w pkt 5.
      4. zapewnienie 12 miesięcznego wsparcia producenta.
      5. przeprowadzenie warsztatu powdrożeniowego przez certyfikowanego inżyniera zgodnie   
         z wymaganiami określonymi w pkt 7.
      6. przeprowadzenie jednego certyfikowanego szkolenia produktowego, przez certyfikowanego inżyniera zgodnie z wymaganiami określonymi w pkt 8.
   2. Oprogramowanie do backupu musi posiadać funkcje monitorujące i raportujące środowisko wirtualne VMware vSphere w wersji 6 lub nowszej, bez potrzeby korzystania z narzędzi firm trzecich. Wymagania minimalne dla tych funkcji opisane są w punkcie 3.
   3. Wraz z Systemem Wykonawca dostarczy 12 miesięczne wsparcie producenta na:
      1. Aktualizacje bazy informacji dotyczących oprogramowania do tworzenia kopii bezpieczeństwa oraz monitorowania i raportowania środowiska do tworzenia kopii bezpieczeństwa i środowiska wirtualnego VMware.
      2. Dostęp do najnowszych wersji dostarczonego oprogramowania oraz wszelkich poprawek i aktualizacji.
      3. Dostęp do bazy wiedzy udostępnianej przez producenta systemu.
      4. Za produkty dostarczane w ramach wsparcia producenta w czasie jego trwania Zamawiający nie będzie ponosił dodatkowych kosztów. Wykonawca dostarczy dokument, w którym producent potwierdza możliwość korzystania przez Zamawiającego z usług wsparcia technicznego producenta na posiadane przez Zamawiającego rozwiązania, o których mowa w pkt. 1.1. oraz 1.2. do dnia zakończenia 12 miesięcznego okresu wsparcia producenta dla dostarczonego oprogramowania.
2. **Minimalne wymagania Zamawiającego w zakresie tworzenia kopii bezpieczeństwa   
   w zwirtualizowanym środowisku VMware.**
   1. System musi być licencjonowany w modelu „ per-CPU”.
   2. System musi obsłużyć 12 procesorów fizycznych zawierających minimum 8 rdzeni na każdy procesor.
   3. System musi obsługiwać środowisko wirtualne VMware vSphere w wersji 6.0 lub nowszej.
   4. System musi współpracować z hostami ESXi zarządzanymi przez VMware vCenter jak   
      i hostami standalone – pojedyncze hosty.
   5. System nie może wymagać instalacji klientów na backupowanych maszynach wirtualnych.
   6. System musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware vSphere.
   7. System musi mieć możliwość instalacji na następujących systemach operacyjnych:
      1. Microsoft Windows Server 2016
      2. Microsoft Windows Server 2012 R2
      3. Microsoft Windows Server 2012
      4. Microsoft Windows Server 2008 R2 SP1
      5. Microsoft Windows Server 2008 SP2

Niezbędne do pracy Systemu licencje (MS Windows 2012 R2) zapewnia Zamawiający.

* 1. System musi mieć możliwość odzyskiwania całej maszyny wirtualnej na pierwotnym lub innym hoście ESXi.
  2. System musi umożliwiać szybkie przywracanie usług przez uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej w zwykłej pamięci masowej.
  3. System musi mieć możliwość odzyskiwania poszczególnych plików maszyny wirtualnej (takich jak VMX) i jej dysków wirtualnych.
  4. System musi wspierać odtwarzanie plików z następujących systemów plików:
     1. Linux (ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs)
     2. BSD (UFS, UFS2)
     3. Solaris (ZFS)
     4. Mac (HFS, HFS+)
     5. Windows (NTFS, FAT, FAT32, ReFS)
  5. System musi oferować portal samoobsługowy, który będzie umożliwiał administratorom systemu backupu przywracanie maszyn wirtualnych, obiektów MS Exchange oraz baz danych Microsoft SQL
  6. System musi umożliwiać indeksowanie plików zawartych w archiwach maszyn wirtualnych   
     z systemem operacyjnym Windows i Linux w celu szybkiego ich przeszukiwania.
  7. System musi korzystać z mechanizmów VSS (Windows Volume Shadow Copy) wbudowanych w najnowsze systemy operacyjne z rodziny Windows.
  8. System musi mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej.
  9. System musi umożliwiać szybkie tworzenie przyrostowych kopii zapasowych poszczególnych maszyn w ramach istniejącego zadania backupu.
  10. System musi dawać możliwość stworzenia środowiska wirtualnego laboratorium dla VMware vSphere, używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
  11. System musi zapewnić możliwość sprawdzenia poprawności wykonania archiwum poprzez odtworzenie maszyny wirtualnej w izolowanym środowisku i jej uruchomienie w środowisku VMware.
  12. System musi umożliwiać tworzenie pełnej kopii syntetycznej, eliminując konieczność okresowego tworzenia pełnych kopii zapasowych dzięki zastosowaniu ciągłego trybu przyrostowego.
  13. System musi umożliwiać automatyczne kopiowanie wszystkich lub wybranych kopii zapasowych maszyn wirtualnych do wybranej awaryjnej pamięci masowej. System musi także dawać możliwość sprawdzania poprawności i korygowania zapewniające dostępność oraz niezawodność dodatkowych kopii zapasowych.
  14. System musi umożliwiać przechowywanie każdej maszyny wirtualnej w osobnym pliku kopii zapasowej.
  15. System musi mieć wbudowane mechanizmy szyfrowania, zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
  16. System musi mieć wbudowaną możliwość replikacji wirtualnych maszyn pomiędzy hostami ESXi oraz w tym możliwość replikacji ciągłej.
  17. System musi umożliwiać tworzenie różnych opcji kopii zapasowych, jak np. tworzenie kopii zapasowych bezpośrednio przez sieć SAN, przez sieć lokalną lub przez mechanizmy I/O hypervisora.
  18. System musi mieć możliwość instalacji centralnej konsoli do zarządzania serwerami archiwizującymi oraz jednoczesnego zarządzania backupami środowiska VMware.
  19. Dostęp do tej konsoli zarządzającej musi być realizowany przez przeglądarkę WWW.
  20. System musi mieć wbudowany mechanizm informowania o pomyślnym lub niepomyślnym zakończeniu procesu archiwizacji poprzez email, zapis do Event Log’u Windows lub wysłanie komunikatu SNMP.
  21. System musi w pełni korzystać z mechanizmów zawartych w VMware vStorage API for Data Protection, a w szczególności być zgodnym z mechanizmem Changed Block Tracking.
  22. System musi integrować się bezpośrednio z posiadanymi przez zamawiającego, macierzami IBM Storwize V7000. Musi zapewniać tworzenie kopii zapasowych   
      z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku Vmware.

1. **Minimalne wymagania Zamawiającego w zakresie monitorowania i raportowania środowiska kopii zapasowych i środowiska wirtualnego VMware.**
   1. System musi zapewnić możliwość monitorowania, raportowania środowiska do tworzenia kopii zapasowych oraz środowiska wirtualizacyjnego opartego na VMware vSphere w wersji 6.0 lub nowszej – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
   2. Narzędzie do monitorowania i raportowania musi być certyfikowane przez VMware   
      i posiadać status „VMWare Ready”.
   3. System musi korzystać z wbudowanych w infrastrukturę VMware mechanizmów monitorowania (VMware API) i nie może instalować na infrastrukturze żadnych agentów.
   4. System musi zapewnić możliwość monitorowania i raportowania o problemach wszystkich elementów infrastruktury VMware takich jak vCenter Server, klastry, hosty, wirtualne maszyny, wirtualne switche, podsystem dyskowy, hardware.
   5. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
   6. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak   
      i pojedynczych wirtualnych maszyn.
   7. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
   8. Dane przesyłane podczas monitoringu powinny być zaszyfrowane i przesyłane przy pomocy protokołu HTTPS.
   9. W systemie powinny się znaleźć wbudowane łącza do bazy wiedzy VMware skorelowane   
      z obsługiwanymi alertami i wydarzeniami.
   10. System musi umożliwiać przedstawienie w formie graficznej całej topologii infrastruktury wirtualnej wraz z zależnościami – od aplikacji do sprzętu.
   11. System musi umożliwiać planowanie wydajności (tzw. capacity planning).
   12. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
   13. Silnik raportowania musi zapewniać bezpieczny dostęp do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji.
   14. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
   15. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
   16. System musi mieć możliwość ustawienia harmonogramu generowania raportów   
       i dostarczania ich do odbiorców w określonych przez administratora interwałach.
   17. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
   18. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz   
       z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
   19. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
   20. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
2. **Harmonogram realizacji.**
   1. W terminie wskazanym w ofercie złożonej w postępowaniu (maksymalnie do 14 dni) od dnia podpisania umowy Wykonawca dostarczy niezbędne licencje zgodnie z wymaganiami Zamawiającego i złożoną ofertą. Dostawa zostanie potwierdzona podpisaniem Protokołu Odbioru Dostawy.
   2. W terminie wskazanym w ofercie złożonej w postępowaniu (maksymalnie do 30 dni) od dnia dostawy zamówienia Wykonawca dokona wdrożenia.
      1. Przeprowadzi instalacje i konfigurację dostarczonego systemu backupu środowiska wirtualnego.
      2. Rozszerzy posiadane przez Zamawiającego licencje na oprogramowanie VmWare.
      3. Skonfiguruje i zoptymalizuje dostarczone oprogramowanie do współpracy   
         z posiadanymi przez Zamawiającego Systemami i oprogramowaniem.
      4. Skonfiguruje monitoring i raportowanie środowiska backupu i środowiska wirtualnego.
      5. Dostarczy szczegółową dokumentację powykonawczą oraz procedury eksploatacyjne i awaryjne zgodnie z wymaganiami określonymi w pkt 6. Zakres dokumentacji i procedur zostanie uzgodniony wcześniej z Zamawiającym.
      6. Zaktualizuje politykę backupu Zamawiającego tak aby uwzględniała dostarczone, zainstalowane i skonfigurowane oprogramowanie.
      7. Przeprowadzi co najmniej jednodniowy (zgodnie ze złożoną ofertą) warsztat powdrożeniowy zgodnie z wymaganiami określonymi w pkt 8, dokładny termin,   
         w którym zostanie przeprowadzony warsztat powdrożeniowy należy uzgodnić   
         z Zamawiającym.
      8. Zakończenie wdrożenia zostanie potwierdzone podpisaniem Protokołu Odbioru Wdrożenia.
      9. W terminie do 30 dni od dnia podpisania umowy Wykonawca przeprowadzi certyfikowane szkolenie produktowe zgodnie z wymaganiami określonymi w pkt 10.
3. **Minimalne wymagania Zamawiającego dotyczące dostarczonej dokumentacji instalacji, konfiguracji i parametryzacji Systemu Backupu.**
   1. Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji umowy charakteryzowały się wysoką jakością, w szczególności:
      1. Czytelną i zrozumiałą strukturą zarówno poszczególnych dokumentów jak   
         i całej dokumentacji z podziałem na rozdziały podrozdziały i sekcje.
      2. Zachowaniem standardów oraz sposobu pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów, oraz fragmentów tego samego dokumentu jak również całej dokumentacji.
   2. Wykonawca przygotuje w szczególności:
      1. Procedury i instrukcje dotyczące instalacji konfiguracji oraz parametryzacji wdrożonego Systemu.
      2. Procedury i instrukcje wykonania kopii bezpieczeństwa i ich odtworzenia.
      3. Procedury i instrukcje aktualizacji i wdrażania poprawek.
      4. Procedury postępowania w razie wystąpienia błędów lub awarii wraz   
         z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji   
         i rozwiązywania zaistniałych problemów,
   3. Każda z procedur powinna zawierać co najmniej następujące dane:
      1. Nazwa.
      2. Opis.
      3. Częstotliwość wykonywania.
      4. Kroki do zrealizowania w procedurze.
      5. Informacje (o ile są znane, jeśli jest ich dużo to przykłady bądź wzorce) na jakie należy zwrócić uwagę w trakcie wykonywania procedury.
      6. Omówienie zawartości komunikatów jeśli są prezentowane.
      7. Kroki jakie należy podjąć w przypadku natknięcia się na nietypowe sytuacje.
   4. Zamawiający wymaga, aby cała dokumentacja, o której mowa powyżej, podlegała jego akceptacji.
4. **Minimalne wymagania Zamawiającego w zakresie świadczenia usług wsparcia technicznego producenta.**
   1. Wsparcie techniczne producenta musi obejmować minimum;
      1. Konsultacje telefonicznych/mailowe w dni robocze w godz. 8:00-20:00,
      2. Zapewnienie dostępu do systemu obsługi zgłoszeń serwisowych SUPPORT (serwis www/mail),
      3. Zapewnienie dostępu do poprawek,
      4. Zapewnienie dostępu do programów dodatkowych objętych licencją danego produktu,
      5. Zapewnienie dostępu do bazy wiedzy o produkcie.
5. **Minimalne wymagania stawiane przez Zamawiającego w zakresie warsztatu powdrożeniowego Systemu Backupu.**
   1. Z wdrażanego u Zamawiającego rozwiązania Wykonawca zorganizuje warsztat powdrożeniowy, który będzie prowadzony przez certyfikowanego inżyniera zaoferowanego rozwiązania, z zakresu administracji wdrożonego Systemu, dla jednej grupy administratorów liczącej do 8 osób, w siedzibie Zamawiającego w Warszawie przy ul. Koszykowej 16 lub Taborowej 33.
   2. Termin warsztatu zostanie uzgodniony z Zamawiającym z co najmniej siedmiodniowym wyprzedzeniem.
   3. Program warsztatu musi obejmować całość zagadnień związanych z czynnościami administracyjnymi z zakresu administrowania wdrożonym Systemem uwzględniając środowisko produkcyjne Zamawiającego i następującą tematykę:
      1. podstawowa i zaawansowana konfiguracja i administracja systemem,
      2. proces monitoringu i raportowania wdrożonego Systemu oraz analizy wydajności Systemu,
      3. proces tworzenia kopii zapasowych,
      4. proces zarządzania zmianami konfiguracyjnymi Systemu,
      5. diagnozowanie i rozwiązywanie problemów związanych z wdrożonym Systemem.
   4. Program warsztatu musi być zgodny z wersją wdrożonego rozwiązania i obejmować omówienie najczęściej występujących awarii oraz sposoby ich usuwania i zabezpieczania się przed nimi.
   5. Warsztat musi trwać minimum 1 dzień roboczy, 6 godzin efektywnych zajęć. Wykonawca może zaoferować przeprowadzenie warsztatu w rozbudowanej, 2-dniowej formule uzgodnionej przed jego rozpoczęciem z Zamawiającym. Rozbudowany warsztat jest traktowany jako dodatkowe kryterium oceny ofert.
   6. Wykonawca zapewni uczestnikom warsztatu materiały szkoleniowe w formie papierowej i elektronicznej.
6. **Minimalne wymagania stawiane przez Zamawiającego w zakresie autoryzowanego szkolenia produktowego z Systemu Backupu.**
   1. Z wdrażanego u Zamawiającego rozwiązania Wykonawca zorganizuje certyfikowane szkolenie produktowe, które będzie prowadzone przez certyfikowanego inżyniera zaoferowanego rozwiązania, z zakresu administracji wdrożonego Systemu, dla jednej grupy administratorów składającej się z 3 osób.
   2. Termin i miejsce szkolenia zostanie uzgodniony z Zamawiającym z co najmniej dwutygodniowym wyprzedzeniem.
   3. Program szkolenia musi obejmować całość zagadnień związanych z czynnościami administracyjnymi z zakresu administrowania wdrożonego Systemu o którym mowa w pkt 1.1 – 1.2.
   4. Szkolenia muszą się odbyć w Warszawie. Wykonawca musi zapewnić sale wykładowe wraz   
      z wyposażeniem i sprzętem niezbędnym do przeprowadzenia szkoleń. Wykonawca zobowiązany jest do zapewnienia obsługi technicznej sprzętu w trakcie szkoleń.
   5. Szkolenie musi się odbywać w dni robocze od poniedziałku do piątku, w godzinach   
      8 – 17.
   6. Szkolenie musi być prowadzone w języku polskim, Zamawiający dopuszcza, aby materiały   
      i prezentacje były w języku angielskim.
   7. Uczestnicy szkolenia muszą otrzymać certyfikat jego ukończenia.
   8. Zamawiający wymaga dostarczenia dla każdego uczestnika szkolenia materiałów szkoleniowych w postaci papierowej i elektronicznej.
   9. Zamawiający wymaga zapewnienia w dniu zajęć, jednego ciepłego posiłku (obiad dwudaniowy) oraz napojów: kawa, herbata, woda mineralna, drobne przekąski   
      (np. ciasteczka, owoce) itp. dla każdego uczestnika.
7. **Minimalne wymagania Zamawiającego dotyczące świadczenia usług wynikających   
   z udzielonej gwarancji.**
   1. Wykonawca udziela gwarancji na prawidłowe, w pełni zgodne z jego przeznaczeniem, funkcjonowanie Systemu objętego wsparciem technicznym producenta, przez okres 12 miesięcy, tj. od daty podpisania protokołu odbioru końcowego.
   2. Czas usunięcia nieprawidłowości wskazanych w zgłoszeniu gwarancyjnym wynosi do 5 dni roboczych od daty zgłoszenia gwarancyjnego pod rygorem naliczania kar umownych na zasadach określonych w Umowie i może ulec wydłużeniu wyłącznie za pisemną zgodą Zamawiającego w przypadku wystąpienia okoliczności niezależnych od Wykonawcy   
      i Zamawiającego.
   3. Udzielone gwarancje nie mogą ograniczać praw Zamawiającego do użytkowania wdrożonego systemu, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego.
8. **Minimalne wymagania Zamawiającego w zakresie oprogramowania wirtualizacyjnego**
   1. Dostarczone oprogramowanie musi umożliwiać integracje z obecnie posiadanym   
      i wykorzystywanym przez zamawiającego środowiskiem serwerowym zwirtualizowanym   
      w oparciu o oprogramowanie Vmware. Wymagane zarządzanie w oparciu o posiadaną przez zamawiającego konsole VMware vCenter Server 6 Standard for vSphere 6.
   2. Dostarczone oprogramowanie musi zapewnić zgodność z oprogramowaniem posiadanym przez Zamawiającego VmWare Vsphere 6 Enterprise Plus.
   3. Oprogramowanie musi być licencjonowane w modelu „ per-CPU”.
   4. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
   5. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
   6. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
   7. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości.
   8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
   9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
   10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
   11. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
   12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 r2, Suse Linux, Ubuntu, Red Hat Enterprise Linux, Debian, CentOS.
   13. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna musi mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak   
       i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum IE i Firefox).
   14. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. musi umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
   15. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
   16. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych   
       i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.
   17. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
   18. Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.
   19. Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.
   20. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich   
       w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
   21. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
   22. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
   23. 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.
   24. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
   25. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory.
   26. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
   27. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej   
       i przestrzeni dyskowej.
   28. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
   29. Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE/40GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
   30. Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
   31. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
   32. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
   33. System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.
   34. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
   35. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch
   36. i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
   37. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
   38. Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.
   39. Platforma wirtualizacji musi w ramach przełącznika sieciowego zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.
   40. Przełącznik rozproszony musi współpracować z protokołem NetFlow.
   41. Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.
   42. Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.
   43. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
   44. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej.
   45. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by   
       w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury.
   46. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług   
       w przypadku awarii poszczególnych elementów infrastruktury.
   47. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
   48. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego   
       i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn.
   49. Rozwiązanie musi posiadać 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.
   50. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
   51. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
   52. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych   
       (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
   53. Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
   54. Rozwiązanie musi posiadać proaktywnie działający mechanizm, który wymigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii.
   55. System musi umożliwiać kontrole dostępu sieciowego do obszarów wrażliwych wirtualnego centrum danych takiego jak DMZ lub serwery z danymi wrażliwymi podlegające zgodności   
       z przepisami PCI lub SOX w obszarze środowiska wirtualnego.
   56. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi oraz wolumenami dyskowymi, bez przerywania pracy usług.
   57. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia (CPU,RAM) serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
   58. Oferowane oprogramowanie musi umożliwiać rozszerzenie posiadanej platformy wirtualnej polegające na dodaniu nowych hostów fizycznych do istniejącej farmy wirtualnej   
       z możliwością migracji hostów między wszystkimi serwerami fizycznymi wchodzącymi   
       w skład farmy, bez obniżenia posiadanego poziomu wsparcia technicznego producenta posiadanego oprogramowania.