Załącznik nr 1
do Umowy 33/ST/SPIS/PN/2019

Opis Przedmiotu Zamówienia - *zmieniony w dniu 11-09-2019 r.*

Przedmiotem zamówienia jest dostawa uniwersalnej infrastruktury sprzętowo-systemowej do Centrum Przetwarzania Danych w Głównym Urzędzie Statystycznym.

Zamówienie jest zamówieniem udzielanym w częściach, z zastrzeżeniem, że procedowanym postępowaniem jest Część I zamówienia, której przedmiotem jest dostawa uniwersalnej infrastruktury sprzętowo-systemowej do Centrum Przetwarzania Danych w GUS

Zamawiający planuje procedowanie odrębnego postępowania, stanowiącego Część II zamówienia, którego przedmiotem będzie wdrożenie uniwersalnej infrastruktury sprzętowo-systemowej w Centrum Przetwarzania Danych w GUS.

Przedmiot zamówienia przedmiotowego postępowania obejmuje 3 zadania:
1. Zadanie I - Dostawa wyspecyfikowanego sprzętu oraz dostawa dodatkowych elementów infrastruktury sprzętowej w tym kabli, jeśli będą niezbędne do prawidłowego wdrożenia;
2. Zadanie II - Dostawa oprogramowania do wirtualizacji;
3. Zadanie III - Dostawa oprogramowania do backupu z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją.

I. Wspólne uwarunkowania realizacji zadań oraz opis posiadanego przez Zamawiającego środowiska

W Centrum Przetwarzania Danych GUS, Zamawiający posiada środowisko serwerowe oparte na systemach operacyjnych MS Windows Server, stanowiącym platformę systemową dla następujących komponentów infrastruktury informatycznej:
- Systemu usług katalogowych bazującego na Microsoft Active Directory w wersji Windows 2012 R2;
- Modułu monitorowania wydajności oraz dostępności aplikacji i usług zbudowanego na bazie systemu Microsoft System Center Operations Manager 2012 R2;
- Modułu zarządzania konfiguracją dla serwerów stworzonego w oparciu o oprogramowanie Microsoft System Center Configuration Manager 2012 R3;
- Systemu poczty Microsoft Exchange 2010;
- Środowisk do wirtualizacji serwerów bazujących na oprogramowaniu VMware vCenter 5.1;
- Serwerów bazodanowych z oprogramowaniem Microsoft SQL Server 2008 oraz 2012.

1. Opis posiadanej infrastruktury sprzętowej

Infrastruktura sprzętowa w Centrum Przetwarzania Danych kształtowała się w latach 2008-2014, w miarę realizacji kolejnych funkcjonalnych projektów SISP.

Zasoby serwerowe w Centrum Przetwarzania Danych w budynku GUS zostały poszerzone o serwery blade HPE rozmieszczone w infrastrukturach blade HP C7000 oraz serwery blade IBM Flex System rozmieszczone w infrastrukturach blade IBM Flex System Enterprise Chassis.

Skonsolidowane środowisko sprzętowe pamięci masowych zostało oparte na bazie macierzy dyskowych SAN HP EVA 4400, SAN HP EVA 8100, SAN HP EVA 8400, SAN NetApp3240 i IBM Storwize V7000.

2. Opis obecnego środowiska zwirtualizowanego

W Centrum Przetwarzania Danych w budynku GUS oprócz środowiska serwerów fizycznych znajdują się trzy współpracujące ze sobą środowiska wirtualizacyjne Vmware, dwa produkcyjne i jedno zarządzające, z oprogramowaniem VMware vSphere w wersji 5.1. Łącznie działa tam 50 hostów fizycznych. Nowa infrastruktura zwirtualizowana powinna umożliwiać integrację z infrastrukturą istniejącą, w szczególności przenoszenie istniejących maszyn wirtualnych z obecnej infrastruktury do nowej.

II. Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę.

1. Zadanie I - Dostawa wyspecyfikowanego sprzętu oraz dostawa dodatkowych elementów infrastruktury sprzętowej w tym kabli, jeśli będą niezbędne do prawidłowego wdrożenia

W ramach Zadania 1 Wykonawca dostarczy do siedziby Głównego Urzędu Statystycznego, w terminie uzgodnionym z Zamawiającym, z zastrzeżeniem dochowania terminu realizacji Umowy, urządzenia w ilościach wyspecyfikowanych w Tabeli 1, zgodnych z opisem w Tabelach 2-8.

Zamawiający wymaga dostarczenie sprzętu wraz ze standardową, dołączaną przez producenta danego urządzenia dokumentacją techniczną w języku polskim lub angielskim oraz instrukcją obsługi, która powinna być w języku polskim.

Zamawiający wymaga dostarczenia sprzętu:
- fabrycznie nowego, nie używanego w innych środowiskach ani projektach,
- wyprodukowanego nie wcześniej niż 6 miesięcy przed dostawą do Zamawiającego,
- będą pochodzić z autoryzowanego kanału sprzedaży producentów zaoferowanych urządzeń,
- nie były w dniu składania ofert przeznaczone przez producenta do wycofania z produkcji,
- będą współpracować z siecią energetyczną o parametrach: 230 V ± 10% , 50 Hz, jednofazowo i być wyposażone w przewody zasilające,
- objętego okresem gwarancyjnym,
- posiadającego najnowszą dostępną w dniu składania ofert wersję oprogramowania.

Wykonawca w treści złożonej oferty oświadczy, że Urządzenia dostarczone Zamawiającemu będą spełniały powyższe wymagania.

Tabela 1. Zbiorcza specyfikacja ilościowa sprzętu dostarczanego w Zadaniu I

Typ sprzętu	Ilość szt.	Numer tabeli
Macierz dyskowa	1	Tabela 2
Urządzenie do backupu dyskowego z deduplikacją	1	Tabela 3
Infrastruktura serwerowo-sieciowa	3	Tabela 4 (Tabela 4.1, 4.2 i 4.3)
Serwer typ 1 (2 procesory po 20 rdzeni)	23	Tabela 5
Serwer typ 2 (2 procesory po 8 rdzeni)	7	Tabela 6
Serwer typ 3 (2 procesory po 16 rdzeni)	3	Tabela 7
Szafa rack	5	Tabela 8

Zamawiający wymaga dostarczenia macierzy dyskowej, wyspecyfikowanej w Tabeli 2, dostarczenia, urządzenia do backupu dyskowego z deduplikacją wyspecyfikowanego w Tabeli 3, infrastruktury serwerowo-sieciowej wyspecyfikowanej w Tabeli 4 oraz dostarczenia serwerów zgodnych ze specyfikacją określoną w Tabelach 5, 6 i 7, z zastrzeżeniem, że procesory serwerów opisanych w Tabeli 5 powinny być wyłącznie dwudziestordzeniowe, procesory serwerów opisanych w Tabeli 6 powinny być wyłącznie ośmiordzeniowe, natomiast procesory serwerów opisanych w Tabeli 7 powinny być wyłącznie szesnastordzeniowe.
Powyższe wymaganie jest konieczne ze względu na licencjonowanie oprogramowania.
Serwery opisane w Tabelach 5, 6 i 7 będą docelowo umieszczone w infrastrukturach serwerowo-sieciowych opisanych w Tabeli 4. Umieszczenie serwerów w infrastrukturze serwerowo-sieciowej nie jest przedmiotem zamówienia procedowanego postępowania.

Zamawiający wymaga dostarczenia dodatkowych elementów infrastruktury sprzętowej w tym wkładek do interfejsów oraz kabli, jeśli będą niezbędne do prawidłowego i efektywnego podłączenie dostarczonego sprzętu do infrastruktury sieci LAN i SAN Zamawiającego.

Tabela 2. Macierz dyskowa - 1 szt.
Opis minimalnych wymagań dla macierzy dyskowej

Lp.	Parametr	Wymagania minimalne
1.	Definicja	Przez **macierz dyskową** Zamawiający rozumie zestaw dysków twardych kontrolowanych przez kontrolery macierzowe i udostępniający wspólną przestrzeń dyskową bez zastosowania zewnętrznych wirtualizatorów. Za pojedynczą macierz nie można uznać rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN.
2.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”. Wymagania dotyczące szafy rack zawiera Tabel 8.
3.	Przestrzeń dyskowa	Macierz musi udostępniać minimum 190 TiB przestrzeni użytkowej w tym: - minimum 87.5 TiB przestrzeni użytkowej zbudowanej w oparciu o dyski w technologii SSD, - minimum 102.5 TiB użytkowej przestrzeni dla danych zbudowanej w oparciu o dyski w technologii SAS 10K Dyski zabezpieczone mechanizmem RAID6, przy czym liczba dysków w tej grupie RAID nie może być większa niż 8 (RAID6 6+2). Wszystkie dyski danej klasy muszą mieć identyczne parametry pojemnościowe i wydajnościowe.
4.	Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę bez wymiany kontrolerów macierzy, do co najmniej 960 dysków twardych, w tym do 480 dysków SSD. Dla zapewnienia najwyższej wydajności, maksymalna konfiguracja macierzy musi wspierać tworzenie wolumenów rozłożonych na wszystkich dyskach macierzy (tzw. wide-striping) i ich jednoczesne, aktywne udostępnianie ze wszystkich kontrolerów macierzy.
5.	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i Nearline SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
6.	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1 lub RAID10, RAID5 lub RAID50 oraz RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, kontroler, zasilacz. Możliwość definiowania różnych poziomów RAID na tych samych dyskach fizycznych. Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, dla uzyskania podobnej wydajności wymagane jest

		zrealizowanie żądanej pojemności większą o 50% liczbą dysków fizycznych. Macierz musi umożliwiać definiowanie globalnych dysków spare lub odpowiedniej zapasowej przestrzeni dyskowej. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare lub odpowiednią zapasową przestrzeń dyskową.
7.	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC. Macierz musi mieć możliwość rozbudowy do czterech kontrolerów macierzowych. Komunikacja pomiędzy wszystkimi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem protokołów FC/Ethernet/Infiniband. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt/zapis) wszystkich wolumenów utworzonych w ramach całego systemu dyskowego. Macierz wyposażona w połączenia dyskowe SAS min.12 Gb/s.
8.	Pamięć cache wbudowana	Macierz musi być wyposażona w minimum 256 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o pamięć typu RAM. Pamięć cache musi mieć możliwość dynamicznego przydziału zasobów dla zapisu lub odczytu. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci cache zapisu kontrolerów) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
9.	Pamięć cache na SSD	Macierz musi umożliwiać rozbudowę przestrzeni cache za pomocą dysków SSD do minimum 8 TiB. Taka przestrzeń, musi być dostępna zarówno dla zasobów blokowych jak i plikowych. Jeżeli taka funkcjonalność nie jest dostępna, należy zaoferować rozwiązanie wyposażone, w co najmniej 1024 GB DRAM cache.
10.	Interfejsy	Macierz musi posiadać co najmniej 24 porty FC 16 Gb/s oraz 4 porty Ethernet 1 Gb/s (porty Ethernet przeznaczone do obsługi protokołów plikowych CIFS i NFS). Musi istnieć możliwość wymiany części portów FC na porty 10 Gb/s Ethernet (obsługa protokołów blokowych iSCSI/FCoE lub plikowych CIFS i NFS). Wszystkie porty FC muszą być wyposażone we wkładki SFP.
11.	Zarządzanie	Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest monitorowanie wydajności

		macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wewnętrznych, grup dyskowych, dysków logicznych (LUN), pojedynczych napędów dyskowych oraz kontrolerów. Konieczne jest analizowanie wymienionych parametrów na bazie danych historycznych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
12.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych. Musi być możliwość zdefiniowania, co najmniej 65 000 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego dysku/wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli funkcjonalność tzw. wide-striping w oferowanej macierzy nie jest dostępna to należy wyposażyć macierz w 50% więcej przestrzeni dyskowej brutto.
13.	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
14.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 2 048 kopii migawkowych per wolumen logiczny i minimum 65 000 wszystkich kopii migawkowych.
15.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID. Musi być możliwość wykonania kopii w innej grupie dyskowej niż dane oryginalne. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
16.	Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te

		muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
17.	Zdalna replikacja danych	Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych infrastruktur (FC, sieci IP). Jeżeli ta funkcjonalność jest dodatkowo licencjonowana, Zamawiający nie wymaga dostarczenia jej w aktualnym postępowaniu.
18.	Ciągła dostępność do danych	Macierz musi umożliwiać uruchomienie replikacji synchronicznej z inną macierzą z tej samej rodziny i zapewniać – w przypadku awarii i całkowitej niedostępności jednej z macierzy – bezprzerwową pracę systemów działających na platformie przetwarzania danych i korzystających z zasobów pamięci masowych. Opisana powyżej obsługa awarii (przełączenie między macierzami) musi odbywać się w sposób automatyczny i transparenty (bez przerywania dostępu do danych) dla korzystających z macierzy hostów. Opisana funkcjonalność musi integrować się z platformą wirtualizacyjną VMware ESX i posiadać certyfikację VMware vSphere Metro Storage Cluster, potwierdzoną wpisem na ogólnodostępnej liście kompatybilności producenta (http://www.vmware.com/resources/compatibility/search.php). Nie dopuszcza się rozwiązania, które wymaga dodatkowych urządzeń do obsługi powyższej funkcjonalności. Jeżeli ta funkcjonalność jest dodatkowo licencjonowana, Zamawiający nie wymaga dostarczenia tej funkcjonalności w aktualnym postępowaniu.
19.	Zarządzanie wydajnością	Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS (możliwość definiowania progów minimalnych i maksymalnych) dla wybranych wolumenów logicznych w zakresie takich parametrów jak: wydajność w IOPS, wydajność w MB/s, opóźnienie w ms. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
20.	Kompresja i deduplikacja danych	Macierz musi umożliwiać kompresję i deduplikację danych na poziomie blokowym. Musi istnieć możliwość uruchomienia kompresji i deduplikacji (niezależnie i łącznie) na poziomie pojedynczych wolumenów logicznych. Kompresja i deduplikacja danych musi odbywać się w locie, przed zapisaniem danych na dyskach macierzy. Musi istnieć możliwość wykonania operacji odwrotnej – wyłączenia

		kompresji i deduplikacji na określonych wolumenach logicznych. Kompresja i deduplikacja nie mogą być realizowane za pomocą zewnętrznego urządzenia lub oprogramowania. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć w wersji nielimitowanej (w tym bez limitu pojemnościowego). Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, to należy wyposażyć macierz w 50% więcej przestrzeni dyskowej brutto.
21.	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania –odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy. Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii.
22.	Dostęp plikowy	Macierz musi umożliwiać udostępnianie danych plikowych po protokołach CIFS (min. SMB v3) i NFS (min. NFS v4). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
23.	Dodatkowe wymagania	Wszystkie opisane funkcje macierzy mają być dostępne w macierzy na dzień składania ofert i być udokumentowane w dokumentacji technicznej.
24.	Replikacja danych	Macierz musi umożliwiać zdalną replikację danych z istniejącymi macierzami w środowisku Zamawiającego HPE 3PAR StoreServ serii 7000 i 8000 z wykorzystaniem wewnętrznych mechanizmów macierzowych.

Tabela 3. Urządzenie do backupu dyskowego z deduplikacją - 1 szt.
Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej.

L.p.	Cecha	Wymagania minimalne
1.	Definicja	Urządzenie musi być kompletnym rozwiązaniem sprzętowym typu „appliance". Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych. Urządzenie powinno być oficjalnie dostępne w ofercie producentów przed ukazaniem się niniejszego postepowania.
2.	Typ obudowy	Urządzenie musi być przystosowane do montażu w szafie rack 19". Wymagania dotyczące szafy rack zawiera Tabela 8.
3.	Przestrzeń dyskowa	Urządzenie musi oferować minimum 360 TiB przestrzeni użytkowej dla danych (bez deduplikacji).
4.	Bezpieczeństwo danych	Dane przechowywane w obrębie podsystemu dyskowego

		urządzenia muszą być chronione za pomocą technologii RAID-6. Urządzenie musi posiadać zapasowe dyski spare, które będą automatycznie włączane do grup RAID w przypadku awarii jednego z dysków produkcyjnych. Urządzenie musi posiadać co najmniej 1 dysk hot-spare na każde 20 dysków produkcyjnych. Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie z standardem NIST SP 800-88 poprzez mechanizm wielokrotnego nadpisania przeterminowanych danych.
5.	Możliwość rozbudowy	Urządzenie musi umożliwiać rozbudowę pojemności użytkowej dla danych (bez deduplikacji) do co najmniej 780 TiB bez uwzględniania mechanizmów protekcji. Rozbudowa pojemności nie może wymuszać rozbudowy lub wymiany kontrolerów urządzenia – rozbudowa musi odbywać się jedynie poprzez instalację nowych dysków i/lub półek dyskowych.
6.	Interfejsy do hostów	Urządzenie musi posiadać dla ruchu produkcyjnego minimum: • 4 porty FC 16 Gb/s z możliwością obsługi każdym portem FC protokołów VTL oraz deduplikacji na źródle, • 4 porty Ethernet 10/25 Gb/s SFP z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle. Do zarządzania musi posiadać minimum 2 porty Ethernet 1 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle, Oferowane urządzenie musi posiadać możliwość obsługi do 8 portów FC 32 Gb/s lub 8 portów Ethernet 10/25 Gb/s lub dowolnej ich kombinacji.
7.	Wydajność	Urządzenie musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu protokołami CIFS/NFS/ VTL co najmniej 22 TB/h (dane podawane przez producenta) oraz co najmniej 41 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta), a także zagregowaną wydajność odtwarzania protokołami CIFS / NFS / VTL co najmniej 18 TB/h (dane podawane przez producenta). Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych. Urządzenie musi pozwalać na jednoczesną obsługę minimum 500 strumieni (zapis danych, odczyt danych, replikacja danych).
8.	Sposób udostępniania zasobów	Urządzenie musi umożliwiać jednoczesny dostęp do całej pojemności urządzenia wszystkimi poniższymi protokołami: • CIFS, NFS i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów Ethernet,

		• VTL i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów FC. Urządzenie musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie urządzenia. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych. Urządzenie musi umożliwiać przyporządkowanie do pojedynczej biblioteki taśmowej minimum 500 napędów oraz 10 000 slotów na taśmy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
9.	Partycjonowanie	Urządzenie musi umożliwiać podział na minimum 60 partycji logicznych w taki sposób, aby każdy z podłączonych systemów backupowych mógł pracować na osobnym urządzeniu logicznym. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
10.	Deduplikacja danych	Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
11.	Replikacja danych	Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. Zarządzanie całym procesem kopiowania danych oraz wszystkimi kopiami musi być możliwy z poziomu oprogramowania

		backupowego. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
12.	Szyfrowanie danych	Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256 realizowaną na poziomie urządzenia przy pomocy certyfikowanego algorytmu zgodnego ze standardem FIPS 140-2 Level 1. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, dostarczenie ich nie jest aktualnie wymagane.
13.	Usuwanie przeterminowanych danych	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych. Musi istnieć możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
14.	Sposób zarządzania	Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym. Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w urządzeniu za pomocą poczty elektronicznej.
15.	Kompatybilność	Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: Veeam, Commvault, Veritas NetBackup, Micro Focus Data Protector, IBM Spectrum Protect, Microsoft SQL, Oracle RMAN i SAP HANA. W przypadku przyjmowania backupów od aplikacji: Veeam, Commvault, Veritas NetBackup, Micro Focus Data Protector, Microsoft SQL, Oracle RMAN i SAP HANA urządzenie musi umożliwiać deduplikację na źródle i przesłanie tylko nowych, unikalnych bloków danych poprzez sieć FC i Ethernet.
16.	Redundancja	Redundantne zasilacze i wentylatory.
17.	Dodatkowe wymagania	Wszystkie opisane funkcje urządzenia mają być dostępne w urządzeniu na dzień składania ofert i być udokumentowane w dostępnej dokumentacji technicznej.

Tabela 4. Infrastruktura serwerowo-sieciowa – 3 szt.
Opis minimalnych wymagań dla infrastruktury serwerowo-sieciowej

Tabela 4.1 Wymagania podstawowe

Lp.	Parametr	Wymagania minimalne
1.	Typ infrastruktury serwerowo-sieciowej	Przystosowana do montażu w szafie typu rack 19", składająca się z jednej lub większej liczby obudów, umożliwiająca instalację minimum 36 serwerów kasetowych dwuprocesorowych z procesorami Intel Xeon Skylake bez konieczności rozbudowy o kolejne elementy sprzętowe. Pojedyncza obudowa wchodząca w skład infrastruktury o wysokości maksymalnej 10U Infrastruktura obsługująca pasmo 40GbE oraz 32Gb FC.
2.	Moduły komunikacyjne LAN	Wyposażona w minimum dwa niezależne moduły komunikacyjne 40GbE. Urządzenia umożliwiające agregację połączeń LAN/FCoE (Fibre Channel over Ethernet) w infrastrukturze i umożliwiające wyprowadzenie sygnałów LAN i FC/FCoE ze wszystkich serwerów z zachowaniem redundancji połączeń. Awaria dowolnego z zainstalowanych modułów nie może powodować utraty komunikacji dla żadnego z serwerów z siecią LAN. Każdy moduł posiadający minimum 8 portów do serwerów (downlink) o sumarycznym paśmie min. 240Gb oraz 8 portów zewnętrznych (uplink) o sumarycznym paśmie 320Gb bez tzw. „oversubscription". Co najmniej 5 z tych portów musi mieć możliwość obsługi sieci 8Gb FC oraz zamiennie 10GbE/40GbE. Aktywne wszystkie porty w każdym module. Dla każdego z dostarczonych modułów należy dostarczyć: 3 wkładki 40 Gb QSFP + MPO SR4 Transceiver. Sumarycznie z infrastrukturą wymagane jest dostarczenie 6 wkładek 40Gb QSFP+ MPO SR4 Transceiver
3.	Moduły Pamięci Masowej	W ramach infrastruktury należy dostarczyć min. 6 półek dyskowych SAS lub 6 macierzy dyskowych FC (dopuszcza się zastosowanie macierzy zewnętrznej), każda umożliwiająca instalację min. 16 dysków 2,5 cala SAS/SATA/SSD. Półki równomiernie rozłożone pomiędzy obudowy na serwery. - z trzema półkami lub trzema macierzami należy dostarczyć min. 24 dyski o sumarycznej pojemności min. 150TB - z trzema półkami lub trzema macierzami należy dostarczyć min. 48 dyski o sumarycznej pojemności min. 300TB Parametry dysków : SAS, 12Gb, SSD Mixed Used (parametr DWPD >=3. Z oferowanymi półkami lub macierzami należy dostarczyć wszystkie niezbędne elementy typu przełączniki, kontrolery FC lub SAS w serwerach oraz odpowiednie kable umożliwiające w każdej obudowie na serwery podłączenie i udostępnienie zasobów dyskowych do co najmniej 6 serwerów Blade. W celu zapewnienia redundancji wymagane są przynajmniej 2 przełączniki SAS lub FC.
4.	Dodatkowa funkcjonalność modułów LAN	Zainstalowane moduły LAN/FC/FCoE w każdej obudowie z funkcjonalnością przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania kasetowego dla poszczególnych wnęk na serwery. Przydzielenie adresów powodujące zastąpienie fizycznych adresów kart konwergentnych

		lub Ethernet na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN w infrastrukturze jak i poprzez dodatkowe oprogramowanie producenta serwerów. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak, aby między wydzielonymi sieciami nie było komunikacji. Musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 100Mb/s do min.10Gb/s, z dokładnością do 100Mb. Każdy moduł pozwalający na podział fizycznego portu w serwerze na 4 niezależne interfejsy logiczne z regulowaną szerokością pasma i oddzielnymi adresami MAC. Wymagane wszystkie niezbędne licencje na opisaną funkcjonalność dla całej infrastruktury blade.
5.	Moduły komunikacyjne SAN FC	Każda z obudów wchodzących w skład infrastruktury wyposażona w min. 2 moduły SAN FC min. 32Gb, posiadające odpowiednią aktywną liczbę portów zewnętrznych FC zapewniających sumaryczną przepustowość w FullDuplex : 192Gb/s dla portów 8Gb/s, 384Gb/s dla portów 16 Gb/s, 768Gb/s dla portów 32Gb/s. Moduły zapewniające redundantne wyprowadzenie z każdego serwera zainstalowanego w obudowie pasma 2x32Gb/s FC (przy zastosowaniu dedykowanej dwuportowej karty FC). Awaria dowolnego z modułów SAN FC 32Gb nie może powodować utraty komunikacji serwera z siecią SAN FC. Każdy moduł SAN FC wyposażony w min. 8 wkładek SFP+ FC 32Gb/s SW. Jako rozwiązanie równoważne dopuszcza się zastosowanie w każdej z obudów min. 2 modułów LAN/FCoE posiadające odpowiednią aktywną liczbę portów zewnętrznych FC zapewniających sumaryczną przepustowość w FullDuplex : 192Gb/s dla portów 8Gb/s, 384Gb/s dla portów 16 Gb/s, 768Gb/s dla portów 32Gb/s. Moduły zapewniające redundantne wyprowadzenie z każdego serwera zainstalowanego w obudowie pasma 2x32Gb FC (przy zastosowaniu dedykowanej dwuportowej karty LAN/FCoE niezależnej od karty do komunikacji z modułami LAN). Każdy moduł LAN/FCoE wyposażony w min. 8 wkładek SFP+ FC 32Gb SW.
6.	Chłodzenie	Każda obudowa wyposażona w komplet redundantnych wentylatorów (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w infrastrukturze. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza (zasilaczy).
7.	Zasilanie	Każda obudowa wyposażona w komplet zasilaczy redundantnych typu Hot Plug. System zasilania musi pracować w trybie redundancji N+N lub N+1, wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. Infrastruktura przystosowana do zasilania jednofazowego.
8.	Moduły zarządzające	Dwa redundantne, sprzętowe moduły zarządzające, moduły typu Hot Plug, umożliwiający podłączenie klawiatury, myszy i monitora. Każdy moduł musi posiadać port USB i port DisplayPort/VGA. Moduły muszą zarządzać chłodzeniem i zasilaniem, a także dokonywać inwentaryzacji sprzętu w infrastrukturze. Muszą komunikować się z modułami zarządzającymi

		serwerów po dedykowanych łączach min.1GbE, niezależnych od kart sieciowych serwera. Nawet awaria wszystkich modułów komunikacyjnych LAN i SAN FC nie może powodować utraty dostępu do modułu zarządzania każdego z serwerów, czyli musi być możliwe m.in. przejęcie konsoli graficznej każdego z serwerów.

Tabela 4.2 Wymagania dla systemu zarządzania infrastrukturą serwerowo-sieciową

Lp.	Parametr	Wymagania minimalne
1.	Zarządzanie	Zarządzanie w oparciu o jednolite oprogramowanie, czyli z jednego panelu o jednym adresie IP. Oprogramowanie musi w sposób graficzny wizualizować stan poszczególnych elementów infrastruktury (stan normalnej pracy, ostrzeżenia, awarie). Musi istnieć możliwość modyfikacji panelu głównego aplikacji poprzez zmianę kategorii systemów, dla których prezentowany jest stan zdrowia/status. Na przykład musi istnieć możliwość zawężenia prezentacji stanu zdrowia tylko do serwerów kasetowych.
2.	Serwery zarządzające	Dwa dodatkowe serwery zarządzające zainstalowane w oferowanej obudowie, ale niezajmujące żadnego z 36 slotów na serwery w infrastrukturze. Oprogramowanie zarządzające działające na tych serwerach musi pracować w trybie wysokiej dostępności HA (High Availability). Awaria dowolnego z serwerów nie może powodować przestoju w pracy oprogramowania zarządzającego ani utraty jakichkolwiek danych. Parametry serwerów zarządzających, spełniające minimalne wymagania wydajnościowe podane przez producenta oprogramowania zarządzającego na publicznie dostępnych stronach. Wymagane wszystkie potrzebne licencje na systemy operacyjne i ewentualnie wirtualizator, potrzebne do uruchomienia oprogramowania zarządzającego. Jeżeli zapewnienie wysokiej dostępności dla systemu zarządzania wymaga dostarczenia współdzielonej macierzy, to taka macierz musi być częścią oferowanego rozwiązania i musi to być macierz niezależna od innych wyspecyfikowanych macierzy czy zasobów dyskowych
3.	Podstawowe funkcje zarządzania	• zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera; • przedstawienie graficznej reprezentacji w formie 3D temperatury w serwerowni z możliwością identyfikacji najgorętszych miejsc do poziomu szafy technicznej lub serwera; • wizualizacja wykorzystania procesorów (CPU), poboru energii przez serwer i temperatury w czasie rzeczywistym. Wymagana możliwość rysowania widoku centrum przetwarzania danych i nanoszenia na niego serwerów i szaf serwerowych; • bezagentowe zarządzanie i monitorowanie stanu urządzeń; • pojedynczy interfejs zapewniający widoki, podsumowanie szczegółowych informacji o sprzęcie i oprogramowaniu układowym zainstalowanym na serwerach; • zebrane dane muszą być udostępniane poprzez interfejs REST API oraz interfejs graficzny użytkownika; • zarządzanie uprawnieniami użytkowników poprzez definiowanie ról.
4.	Sposób zarządzania	Dostęp do aplikacji zarządzającej z serwera zarządzającego lub dowolnego innego miejsca poprzez przeglądarkę internetową (połączenie szyfrowane

		SSL/TLS) bez konieczności instalowania dodatkowego oprogramowania producenta serwera.
5.	Liczba jednoczesnych sesji zarządzania	W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów.
6.	Zdalna identyfikacja	Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego.
7.	Konfiguracja sprzętowa serwera	Zautomatyzowana konfiguracja sprzętowa każdego serwera kasetowego za pomocą profili.
8.	Dodatkowe cechy oprogramowania do zarządzania	• zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera; • przedstawienie graficznej reprezentacji w formie 3D temperatury w serwerowni z możliwością identyfikacji najgorętszych miejsc do poziomu szafy technicznej lub serwera; • wizualizacja wykorzystania procesorów (CPU), poboru energii przez serwer i temperatury w czasie rzeczywistym. Wymagana możliwość rysowania widoku centrum przetwarzania danych i nanoszenia na niego serwerów i szaf serwerowych; • bezagentowe zarządzanie i monitorowanie stanu urządzeń; • pojedynczy interfejs zapewniający widoki, podsumowanie szczegółowych informacji o sprzęcie i oprogramowaniu układowym zainstalowanym na serwerach; • zebrane dane muszą być udostępniane poprzez interfejs REST API oraz interfejs graficzny użytkownika; • zarządzanie uprawnieniami użytkowników poprzez definiowanie ról.
9.	Licencje	Licencje na powyższą funkcjonalność na wszystkie oferowane serwery.

Tabela 4.3 Wymagania dla systemu udostępniania systemów operacyjnych i automatyzacji dla serwerów zainstalowanych w infrastrukturze serwerowo-sieciowej

Lp.	Parametr	Wymagania minimalne
1.	Zarządzanie	Zarządzanie w oparciu o jednolite oprogramowanie, czyli z jednego panelu o jednym adresie IP, zintegrowane z system do zarządzania do pojedynczej infrastruktury serwerowo- sieciowej. Dostęp do aplikacji zarządzającej z serwera zarządzającego lub dowolnego innego miejsca poprzez przeglądarkę internetową (połączenie szyfrowane SSL) bez konieczności instalowania dodatkowego oprogramowania producenta serwera.
2.	Serwery systemu udostępniania	Dwa dodatkowe serwery systemu udostępniania systemów operacyjnych na każdą infrastrukturę serwerową, ponad te opisane w punkcie „serwer do instalacji w infrastrukturze sieciowo-serwerowej", zainstalowane w oferowanej infrastrukturze, ale nie zajmujące żadnego ze slotów na serwery w każdej infrastrukturze. Serwery razem z zainstalowanym oprogramowaniem muszą działać w klastrze niezawodnościowym i zapewniać wysoką dostępność dla systemu operacyjnego i usług na nich zainstalowanych. Oznacza to, że awaria jednego z serwerów nie może zatrzymać pracy całego systemu udostępniania systemów operacyjnych i automatyzacji uruchamiania infrastruktury, przestoju w pracy oprogramowania systemu udostępniania systemów operacyjnych ani utraty danych. W razie awarii jednego z serwerów wszystkie usługi

		systemu muszą być nadal dostępne. Wymagane jest zapewnienie synchronicznej replikacji danych przechowywanych na dyskach lokalnych pomiędzy serwerami. Parametry serwerów systemu udostępniania systemów operacyjnych, spełniające minimalne wymagania wydajnościowe podane przez producenta oprogramowania na publicznie dostępnych stronach. Wymagane wszystkie potrzebne licencje na systemy operacyjne i ewentualnie wirtualizator, potrzebne do uruchomienia oprogramowania systemu udostępniania systemów operacyjnych. Jeżeli zapewnienie wysokiej dostępności dla systemu zarządzania wymaga dostarczenia współdzielonej macierzy, to taka macierz musi być częścią oferowanego rozwiązania, jako element niezależny od innych zasobów dyskowych
3.	Podstawowe funkcje systemu	- Integracja z systemem zarządzania opisanym w Tabeli 4.2 - przechowywanie obrazów systemów operacyjnych VMware, Red Hat Enterprise Linux i SUSE Linux na dyskach serwerów; - automatyczne klonowanie systemu operacyjnego z obrazu przechowywanego przez system i automatyczne udostępnianie ich serwerom produkcyjnym z Tabeli 5, Tabeli 6 i Tabeli 7 poprzez protokół iSCSI w standardzie 10Gb. Wspierane systemy operacyjne to: VMware ESXi 6.0 ,VMware ESXi 6.5, Red Hat Enterprise Linux 7.x, SLES 12 SP1. Poprzez udostępnianie rozumie się uruchamianie serwerów z iSCSI z gotowym systemem operacyjnym z pominięciem procesu instalacji systemu operacyjnego; - nie dopuszcza się instalowania systemu operacyjnego na serwerach zainstalowanych w infrastrukturze serwerowo-sieciowej, system operacyjny musi być uruchomiony z zasobów dyskowych serwera systemu udostępniania systemów operacyjnych - możliwość modyfikacji konfiguracji systemu operacyjnego poprzez skrypty uruchamiane podczas procesu automatycznego udostępniania systemu serwerom opisanym w Tabeli 5, Tabeli 6, Tabeli 7.

Tabela 5. Serwer typ 1 – 23 szt.
Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej.

Lp.	Parametr	Wymagania minimalne
1.	Procesory (ilość i typ)	2 procesory, każdy min. dwudziestordzeniowy, klasy x86-64bit, dla których serwer osiąga wynik nie mniejszy niż 200 punktów w teście SPECrate2017_int_base, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej. Wynik testu musi być potwierdzony przez organizację SPEC i opublikowany na jej oficjalnej stronie internetowej (www.spec.org).
2.	Pamięć RAM	1.5TB LRDIMM DDR4 w modułach min. 64GB. Serwer posiadający minimum 24 sloty na pamięć.
3.	Interfejsy sieciowe	Minimum 2 Interfejsy sieciowe min. 20GbE lub minimum 4 interfejsów 10GbE (CNA, wspierające FCoE – funkcjonalność w standardzie), z możliwością podzielenia każdego interfejsu na min. 3 interfejsy sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe) i kartę FC/FCoE o przepustowości min. 8Gb (posiadającą własny adres WWN). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej

		Dedykowana karta FC lub FCoE min. 2 portowe, 32Gb FC do podłączenia do zewnętrznej macierzy dyskowej FC. Dedykowany kontroler SAS 12G lub FC min.32Gb do podłączenia dysków z modułów pamięci masowych (opisanych w punkcie Moduły Pamięci Masowej)
4.	Kontroler dyskowy	Sprzętowy kontroler do dysków wewnętrznych z 1GB pamięci cache podtrzymywanej bateryjnie.
5.	Dyski twarde	Min. 2 wnęki przygotowane do instalacji dysków twardych typu hot plug. Zainstalowane dwa dyski hot-plug SSD, każdy o pojemności min. 240GB Mixed Use (DWPD>=3).
6.	Sloty PCI-E	Trzy sloty PCIe 3.0,
7.	Porty	1 x USB 3.0 (wewnętrzny) lub 1 x port na kartę SD
8.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2012 R2, 2016, 2019 Red Hat Enterprise Linux (RHEL) 6 i 7 lub Red Hat Enterprise Linux (RHEL) 7 i 8 SUSE Linux Enterprise Server (SLES) 11 i 12 lub SUSE Linux Enterprise Server (SLES) 12 i 15 VMware 6.5 i 6.7
9.	Zarządzanie serwerem	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: - włączenie, wyłączenie i restart serwera; - podgląd logów sprzętowych serwera i karty; - przejęcie zdalnej pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS); - zdalne podłączenie wirtualnych napędów CD/DVD/ISO i FDD; - integrację z Active Directory; - powiadamianie o zdarzeniach za pomocą email'a; - nagrywanie zdalnych sesji graficznych i ich późniejsze odtwarzanie; - wysyłanie zdarzeń do zdalnego serwera syslog; - współdzielenie jednej zdalnej konsoli graficznej przez 5 użytkowników; - wspierane i obsługiwane SSH, TLS - wspierane i obsługiwane zarządzanie RESTfull - zaawansowane zarządzanie poborem energii przez serwer – historia poboru energii, nakładanie limitów (capping) na pobór mocy. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.
10.	Inne	Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.

Tabela 6. Serwer typ 2 - 7 szt.
Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej.

Lp.	Parametr	Wymagania minimalne

1.	Procesory (ilość i typ)	2 procesory, każdy maksymalnie ośmiordzeniowy, klasy x86-64bit, dla których serwer osiąga wynik nie mniejszy niż 107 punktów w teście SPECrate2017_int_base, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej. Wynik testu musi być potwierdzony przez organizację SPEC i opublikowany na jej oficjalnej stronie internetowej (www.spec.org).
2.	Pamięć RAM	1.5TB LRDIMM DDR4 w modułach min. 64GB. Serwer posiadający minimum 24 sloty na pamięć.
3.	Interfejsy sieciowe	Minimum 2 Interfejsy sieciowe min. 20GbE lub minimum 4 interfejsów 10GbE (CNA, wspierające FCoE – funkcjonalność w standardzie), z możliwością podzielenia każdego interfejsu na min. 3 interfejsy sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe) i kartę FC/FCoE o przepustowości min. 8Gb (posiadającą własny adres WWN). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej. Dedykowana karta FC lub FCoE min. 2 portowe, 32Gb FC do podłączenia do zewnętrznej macierzy dyskowej FC. Dedykowany kontroler SAS 12G lub FC min.32Gb do podłączenia dysków z modułów pamięci masowych (opisanych w punkcie Moduły Pamięci Masowej)
4.	Kontroler dyskowy	Sprzętowy kontroler do dysków wewnętrznych z 1GB pamięci cache podtrzymywanej bateryjnie.
5.	Dyski twarde	Min. 2 wnęki przygotowane do instalacji dysków twardych typu hot plug. Zainstalowane dwa dyski hot-plug SSD, każdy o pojemności min. 240GB Mixed Use (DWPD>=3).
6.	Sloty PCI-E	Trzy sloty PCIe 3.0,
7.	Porty	1 x USB 3.0 (wewnętrzny) lub 1 x port na kartę SD
8.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2012 R2, 2016, 2019 Red Hat Enterprise Linux (RHEL) 6 i 7 lub Red Hat Enterprise Linux (RHEL) 7 i 8 SUSE Linux Enterprise Server (SLES) 11 i 12 lub SUSE Linux Enterprise Server (SLES) 12 i 15 VMware 6.5 i 6.7
9.	Zarządzanie serwerem	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: - włączenie, wyłączenie i restart serwera; - podgląd logów sprzętowych serwera i karty; - przejęcie zdalnej pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS); - zdalne podłączenie wirtualnych napędów CD/DVD/ISO i FDD; - integrację z Active Directory; - powiadamianie o zdarzeniach za pomocą email'a; - nagrywanie zdalnych sesji graficznych i ich późniejsze odtwarzanie; - wysyłanie zdarzeń do zdalnego serwera syslog; - współdzielenie jednej zdalnej konsoli graficznej przez 5 użytkowników; - wspierane i obsługiwane SSH, TLS - wspierane i obsługiwane zarządzanie RESTfull - zaawansowane zarządzanie poborem energii przez serwer –

		historia poboru energii, nakładanie limitów (capping) na pobór mocy. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.
10.	Inne	Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.

Tabela 7. Serwer typ 3 - 3 szt.
Opis minimalnych wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej

Lp.	Parametr	Wymagania minimalne
1.	Procesory (ilość i typ)	2 procesory, każdy min. szesnastordzeniowy, klasy x86-64bit, dla których serwer osiąga wynik nie mniejszy niż 160 punktów w teście SPECrate2017_int_base, dla oferowanego modelu serwera w konfiguracji dwuprocesorowej. Wynik testu musi być potwierdzony przez organizację SPEC i opublikowany na jej oficjalnej stronie internetowej (www.spec.org).
2.	Pamięć RAM	64GB LRDIMM DDR4 w modułach min. 16GB. Serwer posiadający minimum 24 sloty na pamięć.
3.	Interfejsy sieciowe	Minimum 2 Interfejsy sieciowe min. 20GbE lub minimum 4 interfejsów 10GbE (CNA, wspierające FCoE – funkcjonalność w standardzie), z możliwością podzielenia każdego interfejsu na min. 3 interfejsy sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe) i kartę FC/FCoE o przepustowości min. 8Gb (posiadającą własny adres WWN). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej Dedykowana karta FC lub FCoE min. 2 portowe, 32Gb FC do podłączenia do zewnętrznej macierzy dyskowej FC. Dedykowany kontroler SAS 12G lub FC min.32Gb do podłączenia dysków z modułów pamięci masowych (opisanych w punkcie Moduły Pamięci Masowej)
4.	Kontroler dyskowy	Sprzętowy kontroler do dysków wewnętrznych z 1GB pamięci cache podtrzymywanej bateryjnie.
5.	Dyski twarde	Min. 2 wnęki przygotowane do instalacji dysków twardych typu hot plug. Zainstalowane dwa dyski hot-plug SSD, każdy 480GB Mixed Use (DWPD>=3)
6.	Sloty PCI-E	Trzy sloty PCIe 3.0,
7.	Porty	1 x USB 3.0 (wewnętrzny) lub 1 x port na kartę SD
8.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2012 R2, 2016, 2019 Red Hat Enterprise Linux (RHEL) 6 i 7 lub Red Hat Enterprise Linux (RHEL) 7 i 8 SUSE Linux Enterprise Server (SLES) 11 i 12 lub

		SUSE Linux Enterprise Server (SLES) 12 i 15 VMware 6.5.
9.	Zarządzanie serwerem	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: - włączenie, wyłączenie i restart serwera; - podgląd logów sprzętowych serwera i karty; - przejęcie zdalnej pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS); - zdalne podłączenie wirtualnych napędów CD/DVD/ISO i FDD; - integrację z Active Directory; - powiadamianie o zdarzeniach za pomocą email'a; - nagrywanie zdalnych sesji graficznych i ich późniejsze odtwarzanie; - wysyłanie zdarzeń do zdalnego serwera syslog; - współdzielenie jednej zdalnej konsoli graficznej przez 5 użytkowników; - wspierane i obsługiwane SSH, TLS - wspierane i obsługiwane zarządzanie RESTfull - zaawansowane zarządzanie poborem energii przez serwer – historia poboru energii, nakładanie limitów (capping) na pobór mocy. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.
10.	Inne	Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.

Tabela 8. Szafa rack szt. 5

Lp.	Opis wymagania / Element	Wymaganie / Wymagany parametr
1.	Wymiary szafy RACK 19"	Szafa RACK 19" zapewniająca 42U wewnętrznego miejsce do instalacji urządzeń. Wysokość max 202cm, szerokość szafy 80cm (min 79cm) , głębokość szafy min. 115cm./max.131cm
2.	Wyposażenie szafy RACK 19"	Szafa wyposażona w: - drzwi przednie perforowane (perforacja min. 80%), wyposażone w zamek - drzwi tylne, dzielone, wyposażone w zamek - ściany boczne (prawa i lewa strona) z zamykane na zamek. - zaślepki montowane bez użycia narzędzi z przodu szafy, pozwalające na zamaskowanie miejsca o wysokości 30U; wysokość pojedynczej zaślepki max 1U - elementy stabilizujące - elementy do uziemienia - zestaw pierścieni/uchwytów typu D - 4 x listwa PDU min. 7.3kVA, każda obsługująca napięcie 220-240V, z podłączeniem IEC-309 32A 1 fazowe, z 36 gniazdami wyjściowymi C13 i 6 gniazd wyjściowych C19

3.	Standardy przemysłowe dla szafy RACK19”	Szafa RACK 19” zgodna ze standardami: - EIA-310 - WEEE - RoHS compliant - UL/CES Certification
4.	Inne	Możliwość instalacji sprzętu o wadze 1360kg (obciążenie statyczne). Dopuszczalne obciążenie podczas przemieszczania/przesuwania szafy 1360kg (obciążenie dynamiczne) bez użycia dodatkowych środków technicznych (wózek, platforma itp.)

2. Zadanie II - Dostawa oprogramowania do wirtualizacji

Przedmiotem Zadania jest dostawa oprogramowania do budowy środowiska zwirtualizowanego (hiperkonwergentnego), dla wskazanej infrastruktury, umożliwiającego wirtualizację serwerów, zasobów dyskowych i sieci.

Wymaganymi elementami zamówienia są:
1) Pakiet VMware Cloud Foundation Advanced lub oprogramowania równoważnego zawierającego funkcjonalność tego pakietu (licencjonowanie na procesor) – 30 sztuk dwu procesorowych serwerów fizycznych,
2) Oprogramowanie VMware vCenter Server lub oprogramowanie równoważne zawierające funkcjonalność tego oprogramowania (licencjonowanie na instancję) – 1 sztuka,
3) 5 letni okres gwarancji zapewniającej możliwość wprowadzania wszelkich poprawek i nowych wersji, które powstaną w tym okresie na całe dostarczone oprogramowanie.

Ze względu na spójność środowiska i zapewnienie niezawodności platformy wirtualizacyjnej oraz uniknięcie zagrożeń mogących powstać na styku produktów różnych producentów całe oprogramowanie wirtualizacyjne musi być kompatybilne i ściśle ze sobą współpracujące. Dostarczone oprogramowanie musi być w wersji najnowszej na dzień złożenia oferty, z uwzględnieniem specyfiki sprzętu Zamawiającego.

Licencjonowanie musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta oprogramowania uaktualnień i poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania. W ramach umowy Wykonawca ma zapewnić udzielanie uprawnień na witrynie producenta oprogramowania wskazanym przez Zamawiającego osobom (pracownikom Zamawiającego) do pobierania kodu zamówionego oprogramowania i kluczy licencyjnych.

Wirtualizowana infrastruktura sprzętowa będzie się znajdować w 3 szafach rack. Infrastruktura będzie składać się z 30 serwerów fizycznych po 2 fizyczne procesory i 1,5 TB RAM każdy, dostarczonych w ramach realizacji Zadania I i opisanych w Tabeli 5 i 6. Podsystem dyskowy podlegający wirtualizacji będzie składać się z dysków SSD, o łącznej pojemności ponad 1 300 TB.

Warunki równoważności dla elementów pakietu VMware Cloud Foundation oraz VMware vCenter Server są następujące:

A. W zakresie wirtualizacji serwerów i zarządzania środowiskiem serwerów wirtualnych

1) Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego;
2) Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM;
3) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych;
4) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM;
5) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych;
6) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe i 3 porty równoległe;
7) Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 12, SLES 11, REHL 7, RHEL 6, Atomic 7, Solaris 11 ,Solaris 10, OS/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, Oracle Linux , CoreOS;

8) Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji;
9) Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych;
10) Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji;
11) 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;
12) Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi;
13) 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;
14) Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP;
15) Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej;
16) Oprogramowanie do wirtualizacji musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE;
17) Oprogramowanie do wirtualizacji musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych;
18) Oprogramowanie do wirtualizacji 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;
19) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernet'owego w razie awarii karty sieciowej;
20) Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN);
21) Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi;
22) Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE, w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi;
23) Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek;
24) Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych;
25) 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;
26) Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie nie większym niż 5 minut
27) Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switch'y) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług;

28) Rozwiązanie musi posiadać natywne mechanizmy szyfrowania podczas przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi;
29) Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury;
30) Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych;
31) Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania;
32) Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa, jak i zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn;
33) 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 serwerów fizycznych lub partycjonowania sieci;
34) 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;
35) 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;
36) Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek;
37) Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 60 TB;
38) Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej;
39) Rozwiązanie musi umożliwiać konfigurację wysokiej dostępności (HA) dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu;
40) Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www, pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe);
41) Oprogramowanie do wirtualizacji musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader;
42) Wirtualizator musi wspierać TPM 2.0. Oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, rozwiązanie gwarantuje, że wirtualizator uruchomił się w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego;
43) Wirtualizator musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny min. Windows 10 oraz min. Windows Server 2016;
44) Rozwiązanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych;
45) Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że z punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego

TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora;

46) Rozwiązanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Taka funkcjonalność powoduje, że w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, eliminowana jest czasochłonna faza inicjalizacji serwera fizycznego – następuje skrócenia czasu wymaganego do ponownego uruchomienia serwera fizycznego podczas operacji aktualizacji;
47) Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich serwerów dostarczonych w ramach postępowania;
48) Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K;
49) Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza, to, że jeśli serwer fizyczny posiada funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizator na podstawie tych danych jest w stanie proaktywnie przenieść wszystkie maszyny wirtualne na inne, prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego;
50) Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej;
51) Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym;
52) 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;
53) Przełącznik rozproszony musi współpracować z protokołem NetFlow;
54) Platforma wirtualizacji powinna 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;
55) Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port;
56) 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;
57) Rozwiązanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju, na poziomie konkretnych maszyn wirtualnych;
58) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. procesorów, pamięci RAM, przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane sprzed roku;
59) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych;
60) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy różnymi Centralnymi Konsolami Zarządzającymi platformy wirtualnej na daleką odległość min. 150 km;

61) Rozwiązanie powinno posiadać proaktywnie działający mechanizm, który przemigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii;
62) Rozwiązanie musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn;
63) Rozwiązanie musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką;
64) Rozwiązanie musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone;
65) Rozwiązanie jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy;
66) Rozwiązanie musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervisor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany);
67) Rozwiązanie musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach;
68) Rozwiązanie musi umożliwiać instalowanie, uruchamianie i zarządzanie aplikacjami Big Data oraz Hadoop z poziomu platformy wirtualizującej;
69) Rozwiązanie musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU do maszyn wirtualnych;
70) Wirtualizator musi wspierać tzw. rozwiązanie trwałej, nieulotnej pamięć (Persistent Memory) zbliżonej do szybkości pamięci DRAM. W ten sposób wirtualizator może udostępnić dla maszyn wirtualnych dyski, które wspierają taką funkcjonalność - ultraszybką pamięć masową zbliżoną do pamięci DRAM;
71) Wirtualizator musi wspierać protokół Remote Direct memory Access (RDMA) poprzez konwergentny Ethernet, lub RoCE (“rocky”) v2, Fiber Channel over Ethernet (FCoE) adapter, i iSCSI rozszerzenie dla RDMA (iSER);
72) Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Centralna konsola graficzna powinna działać jako gotowa, wstępnie skonfigurowana maszyna wirtualna (tzw. virtual appliance);
73) Konsola graficzna musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum IE i Firefox) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem standardu HTML5;
74) Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska;
75) Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną;
76) Rozwiązanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo musi być możliwość ustawienia harmonogramu wykonywania kopii zapasowej.

B. <u>W zakresie wirtualizacji zasobów dyskowych</u>

1) Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD;

2) Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania" operacji odczytu/zapisu (Read/Write IO) po stronie serwerów fizycznych;
3) Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności "w locie";
4) Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania/dodatkowych maszyn wirtualnych;
5) Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną;
6) Narzut definiowany jako moc procesora i zużycie pamięci RAM fizycznego serwera podczas działania rozwiązania tj. podczas udostępniania zasobów dyskowych dla min. 50 maszyn wirtualnych, gdzie każda korzysta z min. 400GB przestrzeni dyskowej i generująca min. 800 IO/sek., nie może być większy niż 10% zasobów fizycznego serwera dostarczonego w ramach postępowania. W przypadku braku oficjalnych testów na stronie producenta rozwiązania Zamawiający zastrzega sobie prawo do przeprowadzenia testów wydajności na etapie analizy ofert oraz odbiorów rozwiązania;
7) Rozwiązanie musi zapewniać możliwość budowy wspólnej wysoko-wydajnej i wysoko-dostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez minimalnie 2 serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 64 serwerów fizycznych;
8) Rozwiązanie musi zapewniać obsługiwanie dysków wirtualnych maszyn do rozmiaru min. 60TB;
9) Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache'ujący, dysk pojemnościowy;
10) Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
11) Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi centami przetwarzania danych, między różnymi szafami rack/chassis;
12) Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną stronę producenta na której znajduje się lista wspieranych lub rekomendowanych konfiguracji. Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawcę/producenta (np. dyski, adaptery, specjalizowane karty i kontrolery);
13) Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej;
14) Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych;
15) Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych;

16) Rozwiązanie musi umożliwiać utworzenie wysokodostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. oddziału zdalnego, zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje. Architektura systemu musi mieć możliwość dołączania kolejnych lokalizacji oddziałów zdalnych w ilości min. 6;
17) Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych;
18) W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) posiadający wbudowane mechanizmy typu Multi-Processor Fault Tolerance;
19) W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) pracujący niezależnie od systemów operacyjnych jakie wspiera;
20) Rozwiązanie musi posiadać na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 4 niezależnych producentów sprzętu serwerowego dostępnego na rynku Unii Europejskiej;
21) Oprogramowanie do wirtualizacji podsystemu dyskowego (SDS) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja), wirtualizacji serwerów (Hypervisor) oraz wirtualizacji sieci IP (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe);
22) Oprogramowanie musi zapewniać natywną integrację (bez skryptów i/lub pluginów) z obecnie używanym przez Zamawiającego systemem zarządzania wirtualnym środowiskiem VMware – Vcenter;
23) Rozwiązanie musi zapewniać możliwość zmniejszania przestrzeni dyskowej (odjęcie pojedynczego dysku, odjęcie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych;
24) Rozwiązanie musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością w locie;
25) Rozwiązanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania/modyfikacji konfiguracji systemu;
26) Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej oraz musi umożliwiać wykorzystanie ww. przestrzeni dyskowej przez serwery fizyczne nie posiadające dysków wewnętrznych;
27) Rozwiązanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych do maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning;
28) Rozwiązanie musi mieć możliwość skonfigurowania dedupikacji i kompresji przy zapisie danych na dysk/grupę pojemnościową (składowanie danych);
29) Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla technologii deduplikacji oraz technologii implementującej RAID5 i RAID6 za pomocą oprogramowania;
30) Rozwiązanie musi umożliwiać utworzenie jednej przestrzeni dyskowej jako „rozciągniętego klastra geograficznego" realizującego scenariusze Disaster Recovery/Disaster Avoidance, zbudowanego w oparciu o dyski wewnętrzne serwerów fizycznych umieszczonych w dwóch różnych lokalizacjach fizycznych, gwarantując tym samym dostępność danych na wypadek awarii całego pojedynczego Data Center oraz dowolnego elementu w dowolnej lokalizacji;
31) Rozwiązanie musi umożliwiać szyfrowanie wirtualnych maszyn zlokalizowanych w zbudowanym w oparciu o rozwiązanie zasobie dyskowym oraz musi umożliwiać szyfrowanie maszyny wirtualnej bez przerywania jej pracy podczas przenoszenia na inny host lub zasób dyskowy.

C. <u>W zakresie wirtualizacji sieci</u>

1) Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) w oparciu o środowiska wirtualne;
2) Oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci protokołów sieciowych;
3) Rozwiązanie realizujące usługi wirtualnych sieci musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub plugin'ów nie wspieranych przez dostawcę platformy wirtualizatora serwerów;
4) Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego przełącznika instalowanego w jądrze wirtualizatora serwerów (Hypervisor), umożliwiający tworzenie logicznych segmentów sieci L2; Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta wirtualizatora serwerów;
5) Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego routera instalowanego w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników;
6) Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN;
7) Oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN oraz niezwirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów;
8) Oprogramowanie musi zapewnić funkcjonalność wirtualnego routera wspierającego protokoły OSPF i BGP. Routing statyczny oraz BGP musi być możliwy poprzez tunel GRE;
9) Rozwiązanie musi posiadać funkcję łączenia (bridge) segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie wirtualnej bramy (bridge);
10) Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT);
11) Rozwiązanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego;
12) Rozwiązanie musi posiadać pełną wymaganą funkcjonalność zarówno funkcji bezpieczeństwa jak i funkcji sieciowych w ramach jednego produktu i być gotowe do instalacji i konfiguracji z wykorzystaniem GUI;
13) Oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API;
14) Zmiana konfiguracji sieciowej musi odbywać się poprzez narzędzia zarządzające dostępne dla środowiska wirtualizacyjnego serwerów;
15) Aktualizacje oprogramowania powinny odbywać się poprzez zintegrowany portal służący do ich planowania i uruchamiania. Portal musi umożliwiać przegląd wszystkich elementów systemu pod kątem ich aktualnej oraz przygotowanej do aktualizacji wersji. Portal musi oferować wskaźniki postępu aktualizacji, umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia spójności działania systemu przed oraz po aktualizacji;
16) Oprogramowanie powinno zapewniać wsparcie dla wykorzystania plików danych JSON oraz XML;
17) Oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisora/wirtualnego interfejsu sieciowego (vNIC), dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewalli;
18) Rozwiązanie musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego w/na poziomie jądra wirtualizatora (Hypervisor) serwerów umożliwiający tworzenie polityk bezpieczeństwa w warstwach 2-4 modelu OSI. Nie dopuszcza się stosowania filtracji typu "reflexive". Wymagana jest możliwość definiowania reguł dla warstwy 7 modelu OSI dla wybranych aplikacji w celu zapewnienia kontroli przepływu danych oraz planowania mikro-segmentacji;

19) Musi zostać zapewniona możliwość tworzenia reguł firewalla w trybie stateless dla różnych grup wirtualnych maszyn;
20) Oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze;
21) Rozwiązanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa. Wymagane min.: nazwa maszyny wirtualnej, nazwa przełącznika wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny;
22) Oprogramowanie realizujące usługę rozproszonego firewalla musi być zarządzane przez narzędzie zarządzające warstwą wirtualną serwerów. Wyklucza się używanie skryptów lub pluginów nie wspieranych przez dostawcę platformy wirtualizatora serwerów;
23) Rozwiązanie musi zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do wirtualnej maszyny po zmianie jej adresu IP;
24) Rozwiązanie musi oferować w ramach platformy, funkcjonalność bezpiecznego, zdalnego i szyfrowanego dostępu użytkowników dla minimum następujących systemów operacyjnych : Windows 7 i wyższe, Mac OS oraz Linux, przy użyciu technologii SSL VPN;
25) Rozwiązanie musi oferować w ramach platformy, możliwość terminowania tuneli IPSec site-to-site z metodą authentykacji współdzielonego klucza (pre shared key) lub certyfikatu;
26) Rozwiązanie musi umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall warstwy 7, m.in. integracja z systemem do zarządzania Next Generation Firewall;
27) Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do rozwiązań firm trzecich z obszaru bezpieczeństwa;
28) Oferowane oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu – tj. load balancing działającą do warstwy 7 modelu ISO OSI:
    a) Rozwiązanie musi zapewniać następujące mechanizmy przywiązania sesji: adres źródłowy, cookie, SSL ID oraz JSessionID,
    b) W ramach inspekcji warstwy 7 rozwiązanie musi oferować funkcję blokowania i modyfikacji URL,
    c) Rozwiązanie musi oferować możliwość wstrzykiwania nagłówka XFF (X-Fowarder-For);
29) Funkcja Wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci;
30) Rozwiązanie typu Identity Firewall musi zapewniać integrację z Active Direcory z obsługą selektywnej synchronizacji;
31) Rozwiązanie musi posiadać funkcję łączenia (bridge) segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika firm trzecich;
32) Rozwiązanie musi zapewniać mechanizm wspomagający planowanie tworzenia grup oraz polityk bezpieczeństwa;
33) Rozwiązanie musi oferować funkcjonalność typu Identity Firewall umożliwiające obsługę sesji użytkowników na pulpitach wirtualnych (VDI) oraz serwerach aplikacji (RDSH) współdzielących pojedynczy adres IP;
34) Rozwiązanie musi oferować funkcjonalność identyfikacji aplikacji, np. MySQL, http, DNS, DHCP, Active Directory, TLS, itp. na poziomie sieciowym OSI warstw 5-7, a następnie móc wykorzystać tę informację w rozproszonym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji;
35) Rozwiązanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) opartych o wirtualizację VMware vSphere;
36) Rozwiązanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego oraz fizycznego;
37) Rozwiązanie musi mieć możliwość wykorzystania wbudowanego kolektora w celach dalszej analizy ruchu;

38) Rozwiązanie musi mieć możliwość tworzenia automatycznych rekomendacji reguł firewalla na bazie zebranych informacji o przepływach;
39) Rozwiązanie musi mieć możliwość wizualizacji ścieżki logicznej i przejść w relacji vm-vm, wskazanie komponentów sieciowych w topologii logicznej i fizycznej (przełączników, routerów, firewalli) oraz połączeń między nimi z uwzględnieniem komponentów wirtualnych;
40) Rozwiązanie musi mieć możliwość wizualizacji przepływów pomiędzy maszynami wirtualnymi i/lub środowiskiem fizycznym pogrupowanych ze względu na sieci wirtualne, podsieci, aplikacje, grupy bezpieczeństwa;
41) Rozwiązanie musi mieć możliwość informowania o tym, jakie reguły firewalla wirtualnego są aktualnie zaaplikowane i aktywne;
42) Rozwiązanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły położone wyżej;
43) Rozwiązanie musi mieć możliwość wizualizacji połączeń maszyn wirtualnych do zasobów dyskowych, połączenia do hosta i wyjścia na zewnątrz do sieci fizycznej;
44) Rozwiązanie do analizy przepływów sieciowych musi posiadać funkcjonalność API.

3. <u>Zadanie III -</u> Dostawa oprogramowania do backupu z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją

Przedmiotem tego Zadania jest dostawa oprogramowania do wykonywania backupu i odzyskiwania danych środowiska wirtualnego z wykorzystaniem urządzenia do backupu dyskowego z deduplikacją opisanego w Zadaniu I w Tabeli 3 oraz uwzględnienie oprogramowania wirtualizacyjnego dostarczonego w ramach Zadania II.

Wymaganymi elementami zamówienia są:
1) Oprogramowanie do wykonywania backupu i odzyskiwania danych dla 30 sztuk dwu procesorowych serwerów fizycznych dostarczonych w Zadaniu I i opisanych w Tabeli 5 i 6 oraz podsystemu dyskowego składającego się z dysków SSD o łącznej pojemności ponad 1 300 TB,
2) 5 letni okres gwarancji zapewniającej możliwość wprowadzania wszelkich poprawek i nowych wersji, które powstaną w tym okresie na całe dostarczone oprogramowanie.

<u>Wymagania dla oprogramowania</u>

1. Wymagania ogólne.
1) Oprogramowanie musi współpracować co najmniej z infrastrukturą wirtualizacyjną VMware w wersji 5.x, 6.x oraz Microsoft Hyper-V 2012 R2, 2016 i 2019. Wszystkie funkcjonalności opisane w tej specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
2) Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3) Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.
4) Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych, wspieranych przez vSphere i Hyper-V.

2. Wymagania podstawowe
1) Oprogramowanie <u>musi być licencjonowanie w modelu “per-CPU”.</u> Wszystkie wymienione poniżej funkcjonalności muszą być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone.
2) Oprogramowanie musi umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
3) Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

4) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
5) Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych w takiej puli.
6) Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
7) Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
8) Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
9) Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki" na wirtualnej maszynie.
10) Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.
11) Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time).
12) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
13) Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
14) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
15) Oprogramowanie 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) Oprogramowanie musi oferować zarządzanie kluczami szyfrowania w przypadku utraty podstawowego klucza.
17) Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).
18) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

3. Wymagania dotyczące wykonywania kopii zapasowych.

1) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
2) Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
3) Oprogramowanie musi oferować powyższy mechanizm z dokładnością do datastore'u.
4) Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.
5) Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
6) Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
7) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

8) Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na oferowanym urządzeniu. Funkcjonalność powinna wspierać łącze sieciowe Ethernet lub FC SAN.
9) Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn do zdalnej lokalizacji z wykorzystaniem wbudowanej akceleracji WAN.
10) Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
11) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
12) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
13) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
14) Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere.
15) Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).

4. Wymagania dotyczące odtwarzania danych i systemów z kopii zapasowych.

1) Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania.
2) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
3) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
4) Oprogramowanie musi umożliwić odtworzenie plików na dowolną maszynę, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
5) Oprogramowanie musi mieć możliwość odtworzenia plików przy pomocy VMware VIX API
6) Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
   a) Linux
      ext3, ext4, JFS, XFS, Btrfs,
   b) BSD
      UFS, UFS2
   c) Solaris
      UFS, ZFS
   d) Windows
      NTFS, FAT, FAT32, ReFS
7) Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Space.
8) Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
9) Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.

10) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
11) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2012 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.
12) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
13) Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux bez konieczności pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
14) Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
15) Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows.
16) Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.

5. Weryfikacja poprawności kopii zapasowych

1) Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowanego środowiska) dla vSphere i Hyper-V, używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
2) Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.

III. Odbiór dostawy urządzeń i oprogramowania.

1. Dostawa urządzeń

1) Odbiorowi podlegać będą wszystkie urządzenia dostarczone w ramach realizacji Zadania I, z zastrzeżeniem, że Zamawiający dopuszcza dostawy częściowe. Odbiór ilościowy dostarczonych elementów zamówienia sprzętowego będzie się odbywał w siedzibie Zamawiającego, w obecności przedstawiciela Zamawiającego i Wykonawcy.
2) Do każdej dostawy Wykonawca dołączy zestawienie dostarczonych urządzeń, z zaznaczeniem typu, numerów fabrycznych i ilości.
3) Warunkiem przyjęcia dostarczonych Urządzeń, jest sprawdzenie ich przez uprawnionego przedstawiciela Zamawiającego, w zakresie zgodności ze złożoną przez Wykonawcę Ofertą oraz warunkami Umowy. Sprawdzeniu podlegać będzie w szczególności: ilość dostarczonych Urządzeń oraz czas (godziny) wykonania dostawy, który powinien uwzględniać wymagania klauzuli środowiskowej. Do każdej dostawy Wykonawca dołączy oświadczenie, potwierdzające, że dostarczone Urządzenia są zgodne z wymaganiami określonymi przez Zamawiającego w Opisie przedmiotu zamówienia oraz Ofertą Wykonawcy.
4) Potwierdzeniem wykonania każdej z dostaw urządzeń, będzie Protokół odbioru dostawy podpisany z wynikiem pozytywnym
5) Po sprawdzeniu dostawy urządzenia zostaną ponownie zapakowane i pozostawione w serwerowniach GUS, tj. w miejscu gdzie będą uruchamiane.
6) Zamawiający wymaga, aby dostarczone przez Wykonawcę urządzenia zostały wyraźnie oznakowane symbolami umowy.

2. Dostawa oprogramowania

1) Odbiorowi podlegać będzie całość oprogramowania określonego dla Zadania II i Zadania III w OPZ.
2) Odbiór oprogramowania nastąpi na podstawie dostarczonych przez Wykonawcę dokumentów licencyjnych wystawionych na Zamawiającego.

3) Warunkiem przyjęcia dostarczonego oprogramowania, jest jego sprawdzenie przez uprawnionego przedstawiciela Zamawiającego, w zakresie zgodności ze złożoną przez Wykonawcę Ofertą oraz warunkami Umowy. Sprawdzeniu podlegać będzie w szczególności ilość dostarczonego oprogramowania oraz czas (godziny) wykonania dostawy, który powinien uwzględniać wymagania klauzuli środowiskowej. Do każdej dostawy Wykonawca dołączy oświadczenie, potwierdzające, że dostarczone oprogramowanie jest zgodne z wymaganiami określonymi przez Zamawiającego w Opisie przedmiotu zamówienia oraz Ofertą Wykonawcy.
4) Potwierdzeniem wykonania każdej z dostaw oprogramowania, będzie Protokół odbioru dostawy, podpisany z wynikiem pozytywnym;

IV. <u>Warunki gwarancji</u>

1. Wykonawca obejmie wszystkie dostarczone, w ramach realizacji Zadania I Urządzenia, dostarczone w ramach realizacji Zadania I, bezpłatną gwarancją przez okres minimum 60 miesięcy, zastrzeżeniem, że okres bezpłatnej gwarancji będzie zgodny z deklaracją Wykonawcy złożoną w formularzu ofertowym.
2. Wykonawca obejmie dostarczone, w ramach realizacji Zadania II i III oprogramowanie, bezpłatną gwarancją przez okres 60 miesięcy.
3. Gwarancja, o której mowa w pkt. 1, będzie obejmować wszystkie komponenty oferowanych Urządzeń, z zastrzeżeniem, że uszkodzone dyski twarde, w przypadku konieczności ich wymiany, pozostają własnością Zamawiającego.
4. Okres gwarancji rozpoczyna się od dnia podpisania przez Strony Końcowego protokołu odbioru z wynikiem pozytywnym.
5. Warunki udzielonej gwarancji będą zgodne z wymaganiami Zamawiającego, z zastrzeżeniem, że nie mogą być gorsze niż warunki gwarancji producenta(ów) Urządzeń i oprogramowania.
6. Udzielona przez Wykonawcę gwarancja nie wyłącza prawa Zamawiającego do gwarancji udzielonych przez producentów Urządzeń i oprogramowania, dostarczonych w ramach realizacji przedmiotu Umowy.
7. W okresie gwarancji udzielonej dla dostarczonych Urządzeń Wykonawca:
   1) zapewni koordynatora obsługi gwarancyjnej, z którym będą prowadzone wszelkie bieżące uzgodnienia w zakresie realizacji napraw gwarancyjnych i przeglądów,
   2) wykona cykliczne przeglądy Urządzeń nie rzadziej niż co 12 miesięcy, przy czym pierwszy i ostatni przegląd powinny być przeprowadzone odpowiednio w pierwszym i ostatnim roku obowiązywania gwarancji,
   3) zapewni Zmawiającemu 300 godzin bezpłatnych konsultacji technicznych dotyczących zaoferowanych Urządzeń, świadczonych w siedzibie Zamawiającego,
   4) zapewni możliwość zdalnych konsultacji (np. e-mail, telefon), dotyczących rozwiązywania problemów występujących podczas obsługi lub funkcjonowania Urządzeń,
   5) uruchomi kanał kontaktowy w formie elektronicznej przez stronę www lub za pomocą poczty elektronicznej lub telefonicznej, umożlwiający zgłaszanie Awarii,
   6) zapewni realizację serwisu gwarancyjnego w języku polskim.
8. Usługi gwarancyjne w zakresie dostarczonych Urządzeń, świadczone będą w miejscu instalacji Urządzeń na następujących warunkach:
   1) Zgłoszenie Awarii będzie możliwe przez 7 dni w tygodniu w godzinach 0:00-24:00 telefonicznie na nr ……., stronę www …… lub za pomocą poczty elektronicznej na adres…… Przez Awarię rozumie się wadę Urządzenia, zdarzenie, w wyniku którego uszkodzeniu uległ jeden (lub więcej) element urządzenia, ograniczający jego wydajność i funkcjonalność i uniemożliwiający Zamawiającemu korzystanie z urządzenia zgodnie z jego Specyfikacją Techniczną/Instrukcją użytkowania;
   2) Czas reakcji (rozumiany jako maksymalny czas, jaki może upłynąć pomiędzy zgłoszeniem Awarii a reakcją Serwisu) na podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nie może przekroczyć 4 godzin od momentu gwarancyjnego zgłoszenia Awarii przez Zamawiającego jeżeli do zgłoszenia doszło do godziny 14:00. W przypadku gwarancyjnego zgłoszenia Awarii po godzinie 16:00 podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nastąpi następnego dnia roboczego w godzinach od 8:00 do 12:00;

3) Usunięcie Awarii i przywrócenie pełnej funkcjonalności Urządzenia wykazującego awarię, zostanie wykonane w terminie 24 godzin od zgłoszenia Awarii, z zastrzeżeniem, że diagnoza problemu wliczana jest w wymagany czas naprawy;
4) W przypadku gdy nie będzie możliwe usunięcie Awarii urządzenia, w miejscu i terminie określonym w pkt. 8 pkt. 3), Wykonawca zobowiązany będzie dostarczyć na czas jego naprawy wolne od wad Urządzenie zastępcze, o parametrach technicznych nie gorszych niż parametry Urządzania wykazującego Awarię;
5) W przypadku, jeżeli Awaria Urządzenia nie zostanie usunięta w terminie 30 dni od dnia jej zgłoszenia przez Zamawiającego oraz w przypadku ponownego wystąpienia awarii Urządzenia po wykonaniu dwóch napraw dotyczących tego samego elementu (zespołu), Wykonawca zobowiązany będzie do wymiany Urządzenia na nowe, o parametrach nie gorszych niż urządzenie podlegające wymianie;
6) Wszelkie koszty związane z naprawami gwarancyjnymi, usuwaniem Awarii, włączając w to koszt części i transportu z i do siedziby Zamawiającego ponosi Wykonawca;
7) Usunięcie Awarii, będzie każdorazowo potwierdzone Protokołem wykonania naprawy, którego wzór stanowi Załącznik nr 10 do Umowy;
8) W przypadku, gdy w Urządzeniach, dokonana zostanie istotna naprawa lub gdy nastąpi jego wymiana na nowe, okres gwarancji na to Urządzenie biegnie na nowo, od daty podpisania Protokołu wykonania naprawy;
9) W przypadku stwierdzenia niezgodności w sposobie realizacji przez Wykonawcę zobowiązań gwarancyjnych, Zamawiający zastrzega sobie prawo do naliczenia kar umownych i potrącenia ich z Zabezpieczenia należytego wykonania umowy, z zastrzeżeniem, że może to nastąpić po zakończeniu okresu realizacji Umowy;
10) W przypadku, jeżeli Wykonawca nie wywiązuje się ze zobowiązań wynikających z gwarancji, Zamawiający może dokonać czynności naprawy we własnym zakresie lub zlecić jej wykonanie osobie trzeciej, a kosztami obciążyć Wykonawcę z wykorzystaniem kwoty zabezpieczenia należytego wykonania umowy, z zastrzeżeniem, że może to nastąpić po zakończeniu okresu realizacji Umowy;
11) Zamawiający ma prawo dokonywania rozbudowy Urządzeń przez wykwalifikowanych pracowników, a także prawo do przemieszczenia zainstalowanych Urządzeń bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne Urządzeń powstałe z winy pracowników Zamawiającego.

9. Usługi gwarancyjne w zakresie dostarczonego oprogramowania, świadczone będą na następujących warunkach:
   1) Wykonawca zapewni dostęp do bazy wiedzy, aktualnych wersji oraz krytycznych poprawek producentów komponentów związanych z bezpieczeństwem i stabilnością działania oprogramowania w całym czasie trwania gwarancji, poprzez wskazanie i udostępnienie odpowiednich stron www;
   2) Wykonawca zapewni wsparcie techniczne w sytuacji zagrażającej stabilnej pracy oprogramowania, w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji;
   3) Wykonawca zapewni wsparcie techniczne w czasie wykonywania przez Zamawiającego planowanych instalacji poprawek, uaktualnień lub nowych wersji oprogramowania w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji;
   4) Wykonawca zapewni wsparcie techniczne, w tym zdalną diagnozę, w przypadku wystąpienia nieprzewidzianych problemów z oprogramowaniem oraz zapewni rozwiązywanie bieżących problemów technicznych związanych z funkcjonowaniem oprogramowania, w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji;
   5) Wykonawca zapewni konsultacje w zakresie eksploatacji, konfiguracji oraz funkcjonalności oprogramowania w formie konsultacji zdalnych (np. e-mail, telefon), lub w miejscu instalacji.
10. Wykonawca zobowiązuje się do bezkosztowego dla Zamawiającego przekazania zobowiązań wynikających z udzielonej gwarancji na rzecz Wykonawcy wybranego w postępowaniu przetargowym, z którym zawarta zostanie umowa na instalację i wdrożenie dostarczonych Urządzeń i oprogramowania, w tym również zobowiązań gwarancyjnych obejmujących wady, które ujawnią się podczas pierwszej instalacji dostarczonych Urządzeń i oprogramowania.
11. Zamawiający przekaże Wykonawcy dane podmiotu realizującego instalację i wdrożenie dostarczonych

Urządzeń i oprogramowania, nie później niż na 14 dni przed dniem, w którym nastąpić powinno przekazanie zobowiązań gwarancyjnych.

12. Wykonawca jest zobowiązany do wykonywania świadczeń gwarancyjnych w pełnym zakresie określonym umową począwszy od dnia jej podpisania do dnia przekazania zobowiązań gwarancyjnych na rzecz podmiotu wskazanego przez Zamawiającego.
13. W przypadku, jeżeli Wykonawca nie przekaże zobowiązań wynikających z udzielonej gwarancji na rzecz Wykonawcy wybranego w postępowaniu przetargowym, z którym zawarta zostanie umowa na instalację i wdrożenie dostarczonych Urządzeń i oprogramowania w terminie określonym w pkt. 11, będzie zobowiązany do ciągłego świadczenia zobowiązań gwarancyjnych przez cały okres trwania gwarancji, o którym mowa w pkt. 1 i pkt. 2, z zastrzeżeniem braku możliwości jej ograniczenia z uwagi na fakt wykonania wdrożenia dostarczonego przedmiotu Umowy przez podmiot trzeci.
14. Okres rękojmi za wady, którego bieg rozpoczyna się w stosunku do przedmiotu Umowy od dnia podpisania z wynikiem pozytywnym Końcowego protokołu odbioru, wynosi 24 miesiące. Zamawiający będzie mógł dochodzić roszczeń z tytułu rękojmi także po terminie określonym w zdaniu pierwszym, jeżeli zgłosił Wykonawcy wadę w ww. terminie.
15. Przekazanie zobowiązań wynikających z udzielonej gwarancji na rzecz podmiotu trzeciego wskazanego przez Zamawiającego pozostaje bez wpływu na okres i zakres udzielonej rękojmi za wady.