Spis treści

Usunięte: 3
Usunięte: 3
Usunięte: 9
Usunięte: 10
Usunięte: 12
Usunięte: 17
Usunięte: 24
Usunięte: 31
Usunięte: 40
Usunięte: 40
Usunięte: 40
Usunięte: 43
Usunięte: 44
Usunięte: 45
Usunięte: 47
Usunięte: 48
Usunięte: 50
Usunięte: 53
Usunięte: 54
Usunięte: 57
Usunięte: 66
Usunięte: 66
Usunięte: 66
Usunięte: 67
Usunięte: 68
Usunięte: 68
Usunięte: 69
Usunięte: 69
Usunięte: 71
Usunięte: 71
Usunięte: 72

Usunięte: 73

1. Definicje używane w dokumencie:

Na potrzeby niniejszego dokumentu przyjęto następujące definicje:

1) **RU** – jednostka wysokości obudowy danego urządzenia i wysokości szafy teleinformatycznej (ang. rack unit), równa 44.45 mm;
2) **dzień roboczy** – poniedziałek, wtorek, środa, czwartek i piątek z wyjątkiem dni ustawowo wolnych od pracy w Polsce;
3) **czas reakcji na zgłoszenie awarii** – czas, który upłynie od momentu zgłoszenia awarii do podjęcia czynności naprawczych ze strony Wykonawcy; nie dotyczy dostarczanego oprogramowania, dla którego obowiązują warunki gwarancji producenta oraz pozycji dla których przewidziana jest wymiana wadliwego towaru na wolny od wad;
4) **czas naprawy/wymiany** – czas liczony od przybycia serwisu po zgłoszeniu awarii liczony do momentu dokonania skutecznej naprawy albo wymiany wadliwego towaru na wolny od wad. Nie dotyczy dostarczanego oprogramowania, dla którego obowiązują warunki gwarancji producenta oraz pozycji dla których przewidziana jest wymiana wadliwego towaru na wolny od wad.
5) **Komponent** – element funkcjonalny składający się na System, np. serwer, macierz blokowa, system wizualizacji.
6) **Licencja** – jeżeli Zamawiający wymaga dostarczenia licencji na korzystanie z oprogramowania, to w braku innych wyraźnych zastrzeżeń, uważa się, że wymagana licencja musi być dostarczona w ramach ceny ofertowej i nie może być ograniczona czasowo i terytorialnie (dotyczy terytorium UE).
7) **System** – oznacza całościowe rozwiązanie obejmujące m.in. urządzenia, oprogramowanie i aplikacje spełniające wymagania opisane w SWZ, które ma być dostarczone i wdrożone przez Wykonawcę w celu realizacji przedmiotu niniejszego Zamówienia.

2. Serwery obliczeniowe

2.1. Serwer – parametry wspólne dla każdego typu serwera

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Obudowa zapewniająca poprawny montaż w szafie teleinformatycznej 19” o głębokości 120 cm wraz z akcesoriami opisanym w podpunkcie poniżej (2). 2) Obudowa musi zostać dostarczona wraz z zestawem szyn i ramieniem porządkującym ułożenie przewodów umożliwiającym pełne wysunięcie serwera do celów serwisowych bez potrzeby odłączania przewodów podłączonych do zasilaczy i kart sieciowych oraz umożliwiającym bezprzerwowe serwisowanie serwera, w tym minimum wymianę dysków oraz wentylatorów i zasilaczy. 3) Obudowa umożliwiająca instalację dysków 2,5” SATA/SAS/NVMe. 4) Obudowa musi umożliwiać instalację co najmniej 8 dysków w rozmiarze 2,5”.
Płyta główna	1) Płyta główna z możliwością zainstalowania dwóch procesorów. 2) Na płycie głównej muszą znajdować się minimum 32 gniazda przeznaczone do instalacji pamięci. 3) Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 4) Płyta główna musi obsługiwać interfejs PCIe 4.0 Jako rozwiązanie równoważne dopuszcza się rozwiązanie spełniające następujące wymagania: 1) Płyta główna z możliwością zainstalowania dwóch procesorów. 2) Na płycie głównej muszą znajdować się minimum 24 gniazda przeznaczone do instalacji pamięci; 3) Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 4) Płyta główna musi obsługiwać interfejs PCIe 4.0
Wbudowane porty	1) Minimum 1 port USB Type-A w standardzie USB 2.0 lub wyższy na przednim panelu serwera. 2) Minimum 1 port USB Type-A w standardzie USB 3.0 lub wyższy na tylnym panelu. 3) Minimum 1 port VGA.
Wentylatory	1) Redundantne typu Hot-Plug.
Bezpieczeństwo	1) Panel przedni zamykany na klucz służący do ochrony przed nieautoryzowanym dostępem do dysków twardych. 2) Funkcja wyłączenia w BIOS funkcji przycisku zasilania. 3) BIOS musi mieć możliwość przejścia do bezpiecznego trybu rozruchowego z funkcją zarządzania blokadą zasilania, zmianą ustawień BIOS, zmianą hasła do BIOS.

	4) Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 5) Wbudowany moduł TPM minimum 2.0. 6) Funkcjonalność włączania i wyłączania portów USB na obudowie. 7) Możliwość wymazania danych z dysków znajdujących się wewnątrz serwera: a) niezależne od zainstalowanego systemu operacyjnego, b) uruchamiane z poziomu systemu zarządzania serwerem. 8) Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. 9) Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego (ang. firmware) przed manipulacją ze strony złośliwego oprogramowania. a) Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B. b) Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). 10) Serwer musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. Jakiekolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi. 11) Dla zapewnienia odpowiedniego poziomu bezpieczeństwa wszystkie pakiety oprogramowania układowego muszą być podpisane cyfrowo za pomocą kryptograficznej funkcji skrótu (ang. hash) SHA-256 z 2048-bitowym szyfrowaniem lub silniejszym. Serwer musi skanować aktualizacje oprogramowania układowego i porównywać ich sygnatury za pomocą wbudowanego w sprzęt łańcucha zaufania.
Karta Zarządzania	Serwer musi być wyposażony w dedykowaną kartę na potrzeby zdalnego zarządzania. Karta musi być niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadać dedykowany port RJ-45 Gigabit Ethernet oraz musi zapewniać: 1) zdalny dostęp do graficznego interfejsu www karty zarządzającej, interfejs www musi być wykonany w standardzie HTML5 2) szyfrowane połączenie (TLS) oraz uwierzytelnienie i autoryzację użytkownika 3) funkcję zdalnego włączenia, wyłączenia, restartu serwera 4) odczyt dzienników zdarzeń (ang. logs) dotyczących serwera 5) podmontowanie zdalnych napędów wirtualnych 6) uruchomienie wirtualnej konsoli z dostępem do myszy i klawiatury 7) wsparcie dla protokołu IPv4 i IPv6 8) wsparcie dla protokołów: SNMP, IPMI2.0, VLAN tagging, SSH, RedFish 9) funkcję zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne muszą być dostępne dla min. 7 dni wstecz

	10) funkcję zdalnego ustawienia limitu poboru prądu przez serwer 11) integrację z Microsoft Active Directory lub LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych 12) obsługę przez minimum trzech administratorów jednocześnie 13) wsparcie dla automatycznej rejestracji w systemie DNS 14) wysyłanie do administratorów wiadomości e-mail z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej 15) zarządzanie bezpośrednie poprzez złącze USB 16) monitorowanie zużycia dysków SSD 17) automatyczne zgłaszanie alertów do centrum serwisowego producenta 18) aktualizacje oprogramowania układowego (ang. firmware) dla wszystkich komponentów serwera 19) przywrócenie poprzednich wersji oprogramowania układowego 20) funkcję eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do/z pliku XML lub JSON 21) funkcję automatycznego tworzenia kopii konfiguracji serwera w oparciu o zdefiniowany harmonogram 22) wykrywanie odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji oprogramowania układowego serwera 23) uruchomienie funkcjonalności umożliwiającej dostęp bezpośrednio poprzez urządzenia mobilne – funkcja konfiguracji oraz monitorowania najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (dostępnej dla systemów operacyjnych Android i Apple iOS) używając jednego z protokołów BLE lub WIFI (dotyczy serwerów typu „A”) 24) zdalne wyłączenia i włączenia portów USB 25) mechanizm bezpiecznego wycofywania z eksploatacji poprzez automatyczne usuwanie poufnych danych w tym minimum: a) konfiguracji BIOS b) konfiguracji kontrolera RAID c) dzienników systemowych d) danych konfiguracyjnych e) wszystkich danych z nośników wewnętrznych (dyski twarde, DCPMM, NVDIMM). Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zmawiającego, to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych i terytorialnych (dotyczy terytorium UE). Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).
System do zarządzania	1) System do zarządzania serwerami wraz z niezbędną licencją, który musi spełniać niżej wymienione wymagania:

	a) Integrację z wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego oprogramowaniem Microsoft Active Directory lub LDAP w zakresie uwierzytelnienia i autoryzacji kont dostępowych b) zarządzanie dostarczonymi serwerami bez udziału dedykowanego agenta c) wsparcie dla protokołów SNMP, IPMI, SSH, Redfish d) uruchamianie procesu wykrywania urządzeń w oparciu o harmonogram e) szczegółowy opis wykrytych systemów oraz ich komponentów f) funkcja eksportu raportu do min. CSV, HTML, XLS, PDF g) funkcja tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu h) grupowanie serwerów w oparciu o kryteria użytkownika i) tworzenie automatycznie grup serwerów w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostały czas gwarancji j) podgląd stanu środowiska zawierający najważniejsze informacje na jego temat k) podsumowanie stanu dla każdego serwera l) szczegółowy status serwera i jego elementów/komponentów m) filtry raportów umożliwiające podgląd wybranych zdarzeń n) integracja z systemem do obsługi zgłoszeń producenta dostarczonej platformy sprzętowej o) możliwość uruchomienia/przechwycenia wirtualnej konsoli serwera p) możliwość podmontowania wirtualnego napędu na zarządzanym serwerze q) kreator umożliwiający dostosowanie akcji dla wybranych alertów r) możliwość importu plików MIB s) możliwość definiowania ról administratorów t) możliwość zdalnej aktualizacji oprogramowania układowego serwerów u) możliwość aktualizacji oprogramowania układowego oparta o wybrane źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) v) możliwość aktualizacji oprogramowania układowego (ang. firmware) bez potrzeby instalacji agenta na serwerze w) możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów x) moduł raportujący pozwalający na wygenerowanie raportu zawierającego co najmniej następujące informacje: i) numery seryjne serwerów ii) konfiguracje poszczególnych serwerów

	iii) wersje oprogramowania wewnętrznego iv) obsadzenie slotów PCI i gniazd pamięci v) informacje o maszynach wirtualnych vi) aktualne informacje o stanie i poziomie gwarancji vii) adresy IP kart sieciowych viii) występujące alerty ix) adresy MAC kart sieciowych x) stan poszczególnych komponentów serwerów y) możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności z) wdrażanie serwerów w oparciu o profile konfiguracji aa) możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między serwerami bb) tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii serwera przez serwis producenta cc) zdalne uruchamianie diagnostyki serwera. 2) System może być zaoferowany jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej. 3) Musi być dostępna dedykowana aplikacja na urządzenia mobilne (wyposażone w system operacyjny Android/Apple iOS) integrująca się z wyżej opisanym systemem do zarządzania (dotyczy serwerów typu „A"). 4) System do zarządzania serwerem musi być zintegrowany z zaoferowanym oprogramowaniem do zarządzania klastrem wirtualizacyjnym (zwanym dalej konsolą wirtualizatora i opisanym w niniejszym dokumencie w punkcie 7.4) i spełniać następujące wymagania: a) możliwość instalowania poprawek podnoszących wersję oprogramowania układowego (ang. firmware) serwera wprost z konsoli wirtualizatora (wymagana zgodność z zaoferowanym oprogramowaniem wirtualizacyjnym) b) instalacja poprawek dla klastra serwerów musi uwzględniać specyfikę pracy tego klastra i brać pod uwagę środowisko wirtualizatora, aby nie wpływać na stan maszyn wirtualnych, tzn. przełączać kolejno aktualizowany serwer w tryb serwisowy, instalować poprawkę, przełączać z powrotem w tryb produkcyjny zanim uruchomi proces na kolejnym serwerze c) konsola wirtualizatora musi prezentować szczegółowe informacje o serwerze takie jak ilość oraz typ komponentu dla co najmniej: a. procesor b. pamięć RAM c. karty I/O d. wentylatory e. dyski pamięci masowej

	d) konsola wirtualizatora musi prezentować informacje wspierające serwisowanie takie jak: a. numer serwisowy/seryjny serwera b. data obowiązywania gwarancji e) informacje sprzętowe i alerty muszą być prezentowane w konsoli wirtualizatora i mogą być używane tak jak inne alerty wirtualizatora w zakresie ustawień powiadomień, potwierdzania przeczytania alertów oraz używania ich w regułach automatyzujących zarządzanie alertami f) konsola wirtualizatora musi pozwalać na ustawienie bazowej konfiguracji dla serwerów (wersje oprogramowania układowego, wersje sterowników) oraz raportowanie odchylenia wersji na poszczególnych serwerach względem konfiguracji bazowej. Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zmawiającego, to musi ona być dostarczona wraz z serwerem w wersji bez ograniczeń czasowych i terytorialnych(dotyczy terytorium UE). Ponadto Zamawiający wymaga, aby żadna z powyższych funkcjonalności nie wymagała okresowego sprawdzania licencji na zewnętrznych systemach (np. producenta).
Diagnostyka	1) Serwer musi być wyposażony w panel LCD dedykowany przez producenta do zaoferowanej obudowy umożliwiający sprawdzenie stanu pracy serwera (umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, zasilania i o temperaturze oraz wyświetlenie tekstu zdefiniowanego przez Zamawiającego (np. nr inwentarzowy, nr serwera)).
Zasilacze	1) Minimum 2 szt., redundantne, typu Hot-Plug, o sprawności Platinum, o mocy zapewniającej poprawną pracę serwera w zaoferowanej konfiguracji przy pracy na połowie zainstalowanych zasilaczy.
Certyfikaty	Certyfikaty potwierdzające zgodność oferowanego modelu serwera z wykorzystywanym lub planowany do wykorzystania w projekcie przez Zamawiającego oprogramowaniem: 1) Microsoft Windows Server min. w wersji 2022 na stronie: https://www.windowsservercatalog.com/ 2) Red Hat Enterprise Linux (RHEL) min. w wersji 9 na stronie: https://access.redhat.com/ecosystem/hardware 3) VMware ESXi min. w wersji 7 na stronie: https://www.vmware.com/resources/compatibility/search.php
Dokumentacja użytkownika	1) Zamawiający wymaga dostarczenia dokumentacji technicznej w języku polskim lub angielskim w wersji elektronicznej.

Kod pola został zmieniony

2.2. Serwer obliczeniowy typu „A”

Zaoferowany serwer musi spełniać wszystkie minimalne wymagania opisane poniżej.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Wysokość 1 lub 2 RU.
Procesor	1) Zainstalowane 2 procesory 32-rdzeniowe, o taktowaniu co najmniej 2.2 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 660 punktów w teście CPU2017 Floating Point Rate. Wynik dla zaoferowanego modelu serwera w konfiguracji z zaproponowanymi procesorami musi być dostępny na stronie www.spec.org 2) Procesor musi obsługiwać interfejs PCIe 5.0.
Pamięć RAM	1) Minimum 2 TB DDR5 RDIMM 4800 MT/s w konfiguracji wypełniającej wszystkie gniazda pamięci na płycie głównej. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM. 2) W przypadku użycia płyty głównej stanowiącej rozwiązanie równoważne wszystkie gniazda pamięci muszą być obsadzone jednakowymi modułami DDR5 4800 MT/s (tego samego typu i pojemności) dającymi łącznie co najmniej 2 TB pamięci. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.
Kontroler RAID	1) Sprzętowy kontroler dyskowy wspierający interfejs PCIe 4.0, z pojemnością cache minimum 4 GB, umożliwiający konfigurację RAID 0, 1, 5, 6, 10, 50, 60 oraz wyposażony w baterię do podtrzymania pamięci cache w przypadku zaniku zasilania. 2) Kontroler musi być zgodny z zaoferowanym oprogramowaniem do wirtualizacji.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 NVMe o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu. 2) Zainstalowane 2 jednakowe dyski NVME SSD Hot-Swap do intensywnego odczytu (ang. read intensive) o współczynniku DWPD minimum 1 i pojemności minimum 960 GB każdy podłączone za pomocą zaoferowanego kontrolera RAID.
Interfejsy sieciowe	1) Dwa interfejsy sieciowe o przepustowości 1 Gb/s Ethernet w standardzie Base-T. 2) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slocie PCIe 4.0, z gniazdami o przepustowości 100 Gb/s Ethernet posiadająca: a) interfejs PCIe 4.0 x16 b) wsparcie dla wirtualizacji SR-IOV oraz VirtIO c) sprzętowe wsparcie dla szyfrowania AES-GCM 128/256 dla protokołów IPSec i TLS, wsparcie dla AES-XTS d) wydajność min. 215 Mpps e) wsparcie dla RoCE Programmable Congestion Control

	f) wsparcie dla IEEE 1588v2 g) sprzętowe wsparcie enkapsulacji i dekapsulacji dla protokołów VxLAN, NVGRE, Geneve h) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. 3) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slocie PCIe lub w slocie z interfejsem OCP 3.0, z gniazdami o przepustowości 25 Gb/s Ethernet w standardzie SFP28, wspierająca również gniazda 10 Gb/s Ethernet w standardzie SFP+, posiadająca: a) wsparcie dla wirtualizacji SR-IOV b) wsparcie dla enkapsulacji i dekapsulacji dla protokołów VxLAN, NVGRE, Geneve c) wsparcie dla RoCE d) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. 3) Karty opisane w pkt. 2) i 3) muszą poprawnie współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu) pochodzącymi od różnych producentów. Obsługa modułów optycznych innych producentów nie może wymagać instalacji dodatkowego oprogramowania lub zmian w konfiguracji karty.

2.3. Serwer obliczeniowy typu „B"

Zaoferowany serwer musi spełniać wszystkie minimalne wymagania opisane poniżej.

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	1) Nie więcej niż 4 RU.
Procesor	1) Zainstalowane 2 procesory 32-rdzeniowe, o taktowaniu co najmniej 2.95GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 87 tysięcy punktów w teście PassMark – CPU Mark (stan na 07.06.2023r.), w konfiguracji dwuprocesorowej, potwierdzony na stronie cpubenchmark.net 2) Procesor musi obsługiwać interfejs PCIe 4.0.
Pamięć RAM	1) Minimum 2 TB DDR4 RDIMM 3200 MT/s w konfiguracji wypełniającej wszystkie gniazda pamięci na płycie głównej. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM. 2) W przypadku użycia płyty głównej stanowiącej rozwiązanie równoważne wszystkie gniazda pamięci muszą być obsadzone jednakowymi modułami DDR4 RDIMM 3200 MT/s (tego samego typu i pojemności) lub DDR5 4800 MT/s (tego samego typu i pojemności), dającymi łącznie co najmniej 2 TB pamięci. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski M.2 SSD o pojemności minimum 480 GB każdy, skonfigurowane w RAID 1, podłączone za pośrednictwem kontrolera zoptymalizowanego pod kątem rozruchu.
Kontroler RAID	1) Sprzętowy kontroler dyskowy wspierający interfejs PCIe 4.0, z pojemnością cache minimum 4 GB, umożliwiający konfigurację RAID 0, 1,

	5, 6, 10, 50, 60 oraz wyposażony w baterię do podtrzymania pamięci cache w przypadku zaniku zasilania. 2) Kontroler musi być zgodny z zaoferowanym oprogramowaniem do wirtualizacji.
Akcelerator Graficzny	1) Zainstalowane 4 karty GPU przeznaczone do wspomagania obliczeń naukowo inżynierskich pojedynczej i podwójnej precyzji spełniające co najmniej wymagania: a) chłodzenie pasywne b) bazowe taktowanie rdzenia minimum 1060 MHz c) taktowanie rdzenia w trybie turbo minimum 1400 MHz d) pamięcią minimum 80 GB typu HBM2e o taktowaniu minimum 1500 MHz e) szerokością szyny pamięci minimum 5120 bitów f) przepustowością maksymalną pamięci minimum 2000 GB/s g) wspierające PCIe 4.0 x16 wraz z lane and polarity reversal h) karty muszą być połączone ze sobą (każda z każdą) szyną dwukierunkową o przepustowości minimum 600 GB/s i) karty muszą gwarantować natywne wspieranie używanego przez zamawiającego modelu programistycznego CUDA j) karty muszą gwarantować natywne wsparcie dla używanego przez zamawiającego pakietu OpenACC k) karty GPU muszą być komponentem oferowanym w oficjalnym kanale producenta serwera i być objęte tą samą gwarancją co cały serwer.
Interfejsy sieciowe	1) Dwa interfejsy sieciowe o przepustowości 1 Gb/s Ethernet w standardzie Base-T. 2) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slocie PCIe 4.0, z gniazdami o przepustowości 100 Gb/s Ethernet posiadająca: a. interfejs PCIe 4.0 x16 b. wsparcie dla wirtualizacji SR-IOV oraz VirtIO c. sprzętowe wsparcie dla szyfrowania AES-GCM 128/256 dla protokołów IPSec i TLS, wsparcie dla AES-XTS d. wydajność min. 215 Mpps e. wsparcie dla RoCE Programmable Congestion Control f. wsparcie dla IEEE 1588v2 g. sprzętowe wsparcie enkapsulacji i dekapsulacji dla protokołów VxLAN, NVGRE, Geneve h. wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. 3) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slocie PCIe lub w slocie z interfejsem OCP 3.0, z gniazdami o przepustowości 25 Gb/s Ethernet w standardzie SFP28, wspierająca również gniazda 10 Gb/s Ethernet w standardzie SFP+, posiadająca: a. wsparcie dla wirtualizacji SR-IOV

	b. wsparcie dla enkapsulacji i dekapsulacji dla protokołów VxLAN, NVGRE, Geneve c. wsparcie dla RoCE d. wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. 4) Karty opisane w pkt. 2) i 3) muszą poprawnie współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu) pochodzącymi od różnych producentów. Obsługa modułów optycznych innych producentów nie może wymagać instalacji dodatkowego oprogramowania lub zmian w konfiguracji karty.

3. Macierz blokowa

Zaoferowana macierz blokowa musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Obudowa przystosowana do zainstalowania w szafie teleinformatycznej 19” o wysokości 2 RU, musi być dostarczona wraz z zestawem szyn montażowych.
Zasoby dyskowe	1) Macierz musi zostać dostarczona w konfiguracji z minimum 19 jednakowymi dyskami 2.5" SSD NVMe Hot-Swap. 2) Dostarczona macierz musi zapewnić pojemność użyteczną minimum 100 TiB. Pojemność użyteczną macierzy należy rozumieć jako pojemność prezentowaną do serwerów i pozwalającą na rzeczywisty zapis danych o tej objętości na macierzy bez uwzględnienia mechanizmów redukcji danych. Pojemność użyteczna to pojemność po odliczeniu wszelkich narzutów związanych z organizacją danych na dyskach takich jak przechowywanie parzystości, sum kontrolnych, danych systemowych, pojemności zapasowej, itp. 3) Dostarczona macierz musi zapewnić przestrzeń efektywną (po zastosowaniu mechanizmów kompresji i deduplikacji) minimum 400 TiB. 4) Osiągnięta przestrzeń min. 400 TiB musi być zapewniona i gwarantowana przez producenta macierzy. Macierz musi posiadać możliwość zapełnienia całej dostarczonej przestrzeni. Jeśli macierz pozwala na zapełnienie tylko części przestrzeni (np. 80%) to pozostająca „pusta - niewykorzystana" przestrzeń nie będzie wliczona w dostarczoną przestrzeń. 5) Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie wydajności minimum 500 tysięcy IOPS z przestrzeni dyskowej (przy założeniach: dla bloku danych o wielkości 4k odczyt 80%, zapis 20% oraz wszystkie operacje losowe). 6) Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie minimum 1900 MiB/s odczytu z przestrzeni dyskowej (nie z cache macierzy). 7) Zastosowane mechanizmy ochrony danych w zaoferowanej konfiguracji muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 1 (jednego) dysku.

	8) W zaoferowanej konfiguracji macierzy należy uwzględnić przestrzeń zapasową lub dyski zapasowe („Hot Spare") według zaleceń producenta macierzy. Minimalnie pojemność jednego dysku lub jeden dysk. 9) Dostarczona macierz musi być rozwiązaniem zaprojektowanym tylko i wyłącznie do dysków SSD lub modułów flash. Dostarczona macierz w żadnej konfiguracji nie może oferować obsługi dysków obrotowych, a co za tym idzie nie może oferować rozbudowy o dyski obrotowe. 10) Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach zainstalowanych wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób aby utrata dowolnego z nich zapewniła ciągłość dostępu do danych. 11) Macierz dyskowa musi umożliwiać stosowanie w niej na potrzeby składowania danych dysków SSD NVMe lub SCM. 12) Wymagane jest szyfrowanie danych na dyskach. 13) Należy dostarczyć niezbędne licencje na całą pojemność macierzy. Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy – konfiguratora / estymatora potwierdzony przez producenta, potwierdzający spełnienie powyższych wymagań, zawierający zarówno proponowaną konfigurację sprzętową z dokładnym wskazaniem numerów producenta („part number") dla wszystkich elementów jak i ich ilości, w tym typów i okresów wsparcia licencji i gwarancji, jak i wynikające z niej parametry pojemnościowe i wydajnościowe.
Kontrolery macierzy dyskowej	1) Macierz musi być wyposażona w minimum 2 kontrolery. 2) Każdy kontroler macierzy musi być wyposażony w co najmniej 576 GB przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu. 3) Kontrolery muszą wspierać jednocześnie ruch - blokowy i plikowy (wymagane co najmniej protokoły: iSCSI, FC oraz plikowy CIFS - minimum SMB w wersjach 1,2,3,3.1.1, FTP, SFTP oraz NFS). Nie dopuszcza się realizacji funkcjonalności ruchu plikowego za pomocą dodatkowych/zewnętrznych urządzeń. 4) Kontrolery muszą działać w sposób redundantny - tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych - praca w trybie Active/Active. 5) W przypadku awarii zasilania dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania. 6) Obszar pamięci cache przeznaczony do zapisów danych (ang. write cache) musi posiadać lustrzaną kopię (ang. mirror) i poprawnie funkcjonować nawet w razie awarii jednego z kontrolerów macierzy. 7) Każdy kontroler macierzy musi być wyposażony w wielordzeniowe procesory (minimum 48 rdzeni łącznie). 8) Macierz musi umożliwiać obsługę różnych poziomów RAID, co najmniej RAID5, RAID6.
Interfejsy	1) Minimalnie macierz musi być wyposażona w następujące działające porty:

	a) 4 porty 100 Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduł optyczny QSFP28 b) 8 portów 25Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduł optyczny SFP28 c) 2 porty 1 Gb/s Ethernet Base-T do zdalnego zarządzania kontrolerem d) 4 porty minimum 100 Gb/s do podłączania półek dyskowych po protokole NVMe. 2) Interfejsy optyczne opisane w punkcie 1) muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu) pochodzącymi od różnych producentów. 3) Musi być zapewniona możliwość rozbudowy macierzy o minimum 4 dodatkowe porty 100 Gb/s Ethernet jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów.
Redukcja danych	1) Macierz musi zapewniać mechanizm kompresji i deduplikacji danych w trybie „in-line”. Kompresja i deduplikacja muszą być integralną częścią systemu macierzowego bez możliwości zatrzymania bądź wyłączenia przez administratora. 2) Dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne dla wszystkich rodzajów przechowywanych danych (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności). 3) Wymagane jest zagwarantowane przez producenta oferowanej macierzy osiągnięcie współczynnika redukcji danych dla całej macierzy na poziomie min. 4:1 przy spełnieniu wymagań pojemnościowych określonych w punkcie *Zasoby dyskowe*. Zamawiający dopuszcza możliwość dostarczenia macierzy o gwarantowanym przez producenta współczynnika redukcji danych dla całej macierzy w niższym stopniu, jednak w takim przypadku należy dostarczyć macierz w takiej konfiguracji aby przestrzeń efektywna wynosiła min. 400 TiB. W powyższej kalkulacji nie będzie wymagane uwzględnienie danych wcześniej zaszyfrowanych (z pominięciem mechanizmu szyfrowania przez macierz) i wcześniej skompresowanych. 4) Obowiązkowe jest dodanie do oferty odpowiedniego dokumentu zawierającego najlepsze praktyki dotyczące konfiguracji i zarządzania macierzą dostępne online na stronach producenta. 5) Wymagane jest dostarczenie przez Zamawiającego wraz z ofertą potwierdzenia/oświadczenie producenta, że zaoferowana macierz w zaoferowanej konfiguracji sprzętowej będzie oferowała efektywną przestrzeń o pojemności min. 400 TiB. W sytuacji gdy do uzyskania efektywnej przestrzeni będzie wykorzystywany współczynnik redukcji danych, informacja taka musi znajdować się na dostarczonym oświadczeniu.

	Jeżeli takie potwierdzenie/oświadczenie Producenta oferowanej macierzy nie zostanie przedstawione Zamawiającemu do dnia odbioru przedmiotu zamówienia zostanie to zinterpretowane jako brak wymaganego współczynnika redukcji danych. W takim przypadku oferent zobowiązuje się dostarczyć powierzchnię 400 TiB przestrzeni użytecznej zbudowaną z tych samych elementów.
Funkcjonalności	1) Macierz musi umożliwiać wykonywanie procesu aktualizacji oprogramowania układowego (ang. firmware) macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. 2) Macierz musi umożliwiać skalowalną rozbudowę on-line do co najmniej 8 kontrolerów zarządzanych z jednej konsoli oraz poprzez dodawanie półek dyskowych do par kontrolerów. Po takiej rozbudowie musi być możliwość zaprezentowania każdego wolumenu logicznego LUN przez dowolny z kontrolerów bez przerywania dostępu do danych. 3) System musi obsługiwać natywną integrację ze środowiskiem wirtualizacyjnym, dostarczanym w ramach tego postępowania, umożliwiając przypisanie do podsystemu pamięci masowej operacji wirtualizatora, takich jak: a) tworzenie dysków wirtualnych b) klonowanie dysków wirtualnych c) wykonanie kopii migawkowych d) przenoszenie dysków wirtualnych. 4) Macierz musi obsługiwać funkcję „Local Protection” (Snapshot z technologią Redirect-On-Write dla danych blokowych i plikowych i Thin Clones), rozwiązania, które nie obsługują funkcji „redirect on write” nie są dozwolone. Rozwiązanie powinno obsługiwać ciągłą ochronę danych dla dostarczanego wirtualizatora. 5) Macierz musi obsługiwać kopie spójności aplikacji z replikacjami lokalnymi. 6) Zamawiający wymaga dostarczenia licencji dla replikacji zdalnych na etapie postępowania. 7) Macierz musi zapewniać: a) monitorowanie wydajności (opóźnienie, IOPS, odczyt/zapis, szerokość pasma, rozmiar IO, długość kolejki), b) monitorowanie pojemności (łącznie, oszczędność - redukcja danych, snapshoty) c) konfigurację umożliwiającą przekierowanie powiadomienia na adres e-mail d) dostęp poprzez dedykowaną do tego celu aplikacje producenta macierzy dla urządzeń mobilnych (Android i iOS). Rozwiązanie musi być hostowane w środowisku producenta macierzy i być udostępnione bez dodatkowych kosztów przez cały okres użytkowania dostarczonego rozwiązania i zapewniać co najmniej 1 rok danych historycznych.

	8) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych dla aplikacji wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: a) Microsoft Exchange 2016 i 2019 b) SQL Server 2017 i 2019 c) Oracle Databases 18 i 19 d) blokowych i plikowych zasobów dla dostarczonego oprogramowania do wirtualizacji mocy obliczeniowej. Spójność kopii rozumieć należy jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. 9) Macierz zarówno na poziomie jednej macierzy, jak i klastra, musi być zarządzana z poziomu jednej aplikacji, dostarczonej przez jej producenta. Nie dopuszcza się dzielenia zarządzania pomiędzy różne aplikacje. 10) Macierz musi obsługiwać co najmniej dwukierunkową asynchroniczną zdalną replikację przez IP z opcją ustawienia relacji do: "1:1", "1:n", i "n:1". 11) Macierz musi zapewniać mechanizm „thin provisioning”, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą oferowaną pojemność macierzy w wersji bez ograniczeń czasowych. Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez Zmawiającego to musi ona być dostarczona wraz z macierzą w wersji bez ograniczeń czasowych
Zasilanie	1) Macierz musi być wyposażona w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwany dostęp do wolumenów dyskowych (LUN) oraz działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
Dodatkowe wymagania	1) Rozwiązanie musi mieć możliwość rozbudowy do 432 rdzeni procesora oraz minimum 8TB pamięci RAM. Rozbudowa nie może powodować wymiany zastosowanych dysków twardych. 2) Pamięć Write Cache musi być zabezpieczona dwoma bateriami, tak aby w razie awarii jednej baterii, pamięć cały czas miała bateryjną ochronę podtrzymania zasilania. 3) W przypadku instalacji z dwoma macierzami, macierz oferuje możliwość replikacji wolumenu w trybie synchronicznym w taki sposób, aby możliwy był jednoczesny zapis i odczyt z obu replikowanych wolumenów na obu macierzach w tym samym momencie co najmniej dla oferowanego oprogramowania do wirtualizacji zasobów serwerowych. Dodatkowo w razie całkowitej utraty jednej z macierzy, powinny zadziałać mechanizmy wysokiej dostępności w taki sposób, aby dostęp do wolumenu był nieprzerwany z punktu widzenia serwerów korzystających z zasobów macierzy. Funkcjonalność

	musi być integralną cechą macierzy lub może być realizowana za pomocą dodatkowych urządzeń. Replikacja synchroniczna między macierzami musi odbywać się za pomocą protokołu IP. 4) Macierz musi posiadać natywne wsparcie dla technologii NVMe-over-TCP.
Wymiana dysków	1) Wymiana dysków może być dokonywana samodzielnie przez zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski.

4. System szybkiej pamięci masowej o dostępie plikowym

Zaoferowany system szybkiej pamięci masowej o dostępie plikowym musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie plikowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out" (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Rozwiązanie musi być zbudowane na dyskach SSD NVMe nie większych niż 3,84 TB. 4) Architektura systemu oraz zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 2 (dwóch) dowolnych dysków jednocześnie lub 1 (jednego) dowolnego węzła. 5) Wymagane mechanizmy ochrony przed awarią dysku to RAID lub kodowanie nadmiarowe (ECC). W przypadku mechanizmu RAID, ze względu na dłuższy czas odbudowy, macierz powinna być odporna na jednoczesną awarię co najmniej 3 (trzech) dowolnych dysków (należy uwzględnić w konfiguracji pojemności przestrzeni użytecznej). 6) Rozwiązanie musi umożliwiać ochronę danych przy pomocy wielokrotnego zapisu (ang. mirroring). 7) Musi istnieć możliwość zmiany protekcji danych przy zachowaniu nieprzerwanej dostępności zasobów, również pomiędzy trybem ECC i mirroring, w tym również dla plików w obrębie tego samego folderu, bez konieczności ich przenoszenia na inny zasób. 8) W przypadku awarii dysku czas odbudowy nie może być dłuższy niż 60 godzin (w sytuacji braku obciążenia przez urządzenia klienckie). 9) System musi udostępniać całą dostępną przestrzeń w ramach jednego ciągłego systemu plików, który musi być skalowalny do co najmniej 4000 TiB powierzchni użytkowej. 10) System musi umożliwiać rozbudowę do co najmniej 200 węzłów w ramach tego samego systemu dyskowego, prezentujących do klientów jeden system plików. 11) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: a) dysków b) interfejsów sieciowych c) kontrolerów (węzłów)

	d) zasilaczy e) wentylatorów. 12) Dostarczony system musi zapewnić pojemność użyteczną minimum 294 TiB. Pojemność użyteczną należy rozumieć jako pojemność prezentowaną do serwerów i pozwalającą na rzeczywisty zapis danych o tej objętości na macierzy bez uwzględnienia mechanizmów redukcji danych. Pojemność użyteczna to pojemność po odliczeniu wszelkich narzutów związanych z organizacją danych na dyskach takich jak przechowywanie parzystości, sum kontrolnych, danych systemowych, pojemności zapasowej, itp. 13) System musi zapewniać wydajność: a) wydajność nie mniejsza niż 3500 MB/s (megabajtów na sekundę) w przypadku losowych odczytów protokołem NFS v.3 (RFC 1813) dla bloku o wielkości 4KB i nie więcej niż 60 jednoczesnych wątków (ang. threads) na węzeł, b) wydajność nie mniejszą niż 450tys. file OPS (operacji plikowych na sekundę) w teście SPEC SFS 2014 dla obciążenia zdefiniowanego jako SWBUILD przy zachowaniu średnich opóźnień nie większych niż 8ms. Oferent musi przedstawić wyniki testu potwierdzające spełnienie tego warunku, potwierdzone przez producenta sprzętu. 14) System musi być zbudowany z co najmniej 12 jednakowych węzłów (kontrolerów), gdzie każdy realizuje dostęp plikowy do danych i zapewnia wysoką wydajność dostępu do zgromadzonych plików w systemie.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 1 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w 2 procesory klasy x86-64, z których każdy posiada minimum 10 rdzeni. 4) Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci podręcznej (ang. cache) w oparciu o dyski SSD. 5) Każdy z elementów systemu musi być wyposażony w redundantne zasilacze zapewniające odporność na awarię pojedynczego źródła zasilania. 6) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet, każda z nich musi posiadać 2 porty 100 Gb/s Ethernet QSFP28.

	Interfejsy z jednej karty muszą być przeznaczone na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end”). Interfejsy drugiej karty muszą być przeznaczone do zapewniania dostęp do danych (interfejsy typu „front-end”). 7) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end”. 8) Komunikacja pomiędzy węzłami („back-end”) musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end”), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end”), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end”). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego. Zmawiający nie dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC” (ang. Direct Attach Cable). 9) Dostarczony system musi umożliwiać rozbudowę do min. 60 węzłów bez konieczności rozbudowy o dodatkowe przełączniki sieciowe dla połączeń wewnętrznych („back-end”) pomiędzy węzłami. 10) System musi zapewnić gwarantowaną ochronę przed tzw. „cichym uszkodzeniem danych" (ang. silent data corruption) dla wszystkich technologii dyskowych. 11) System musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia dowolnego z elementów urządzenia. Musi posiadać zaimplementowany system jednoznacznego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej przy uszkodzonym dysku. 12) System musi zapewniać pracę jednocześnie wszystkich węzłów w trybie aktywny/aktywny w celu zapewnienia niezawodności i dostępności danych (tzn. każdy kontroler powinien umożliwiać dostęp do wszystkich danych oraz prezentować spójny widok systemu plików).

Pamięć RAM	1) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 4608 GB (tzn. min. 384 GB dla pojedynczego węzła).
Funkcjonalność	1) System musi umożliwiać dynamiczne rozszerzanie i zmniejszanie udostępnianych systemów plików bez konieczności: a) modyfikacji już zainstalowanych węzłów, b) ręcznej migracji/dystrybucji danych na nowe dyski systemu. 2) System musi zapewniać dostęp z rożnych systemów operacyjnych (wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: UNIX, macOS, Linux, Windows) z wykorzystaniem standardowych protokołów. Wymagana jest poprawna obsługa co najmniej: NFS v3 i v4, SMB (CIFS) v2 i v3, FTP, HTTP i S3 API. 3) System musi wspierać natywnie Hadoop Distributed File System (HDFS). 4) Jednoczesny dostęp do tych samych danych musi być możliwy przy wykorzystaniu wszystkich protokołów wymienionych powyżej. System musi również umożliwiać zarządzanie uprawnieniami użytkowników w dostępie wieloprotokołowym. 5) System musi zapewnić obsługę alertów i umożliwiać monitorowanie za pomocą protokołu SNMP (w wersji min. 2c). 6) System musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 7) System musi posiadać funkcjonalność asynchronicznej replikacji danych z wykorzystaniem protokołu TCP/IP celem dystrybucji treści i zapewnienia kopii danych w zdalnej lokalizacji. 8) System musi posiadać funkcjonalność wykonywania kopii migawkowych (ang. snapshot) oraz pozwalać stworzenie co najmniej 1000 kopii migawkowych dla danego katalogu w celu zapewnienia lokalnej ochrony danych. 9) System musi obsługiwać funkcjonalność realizacji kopii zapasowej (ang. backup) za pomocą protokołu NDMP. 10) System musi posiadać wbudowaną funkcjonalność definiowania limitów ilości danych (tzw. quoty) dla wybranych katalogów, użytkowników oraz grup użytkowników. 11) System musi posiadać mechanizm dystrybucji połączeń pomiędzy węzłami (ang. load-balancing) bez potrzeby stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. Load-balancing musi być dostępny i być wspierany zarówno dla protokołów plikowych, jak i dla obiektowych (S3 API).

	12) Administracja systemem musi odbywać się poprzez interfejs graficzny dostępny przez przeglądarkę internetową (poprawna obsługa przez przeglądarki co najmniej Google Chrome i Mozilla Firefox) oraz wiersz poleceń (ang. Command Line Interface, CLI). Musi również istnieć możliwość zarządzania przy pomocy interfejsu programistycznego REST API. 13) Rozwiązanie musi udostępniać statystyki historyczne z wykorzystania systemu i zapewniać statystyki wykorzystania zasobów przez użytkowników oraz generowanie raportów graficznych, w tym raportów porównujących dostępne parametry systemu. 14) System musi posiadać funkcjonalność automatycznego „tiering-u", tzn. przesuwania danych w zależności od ich utylizacji pomiędzy warstwami dyskowymi (ang. tiers), w ramach jednego systemu plików i według polityk ustawionych przez administratora. Dostęp w trybie odczyt/zapis do danych musi być zachowany cały czas, również w trakcie operacji przenoszenia danych (ang. tiering), czy zmiany poziomu protekcji danych (np. z n+1 na n+2) (ang. re-striping). 15) System musi posiadać funkcjonalność monitorowania wydajności (obciążenie CPU lub interfejsów sieciowych, opóźnienia, ilość operacji na sekundę, wydajność per protokół itp.) oraz analityki systemu plików („capacity planning", zmiany na systemie plików). 16) System musi posiadać wbudowaną funkcjonalność audytu, która daje co najmniej możliwość precyzyjnego określenia użytkownika odpowiedzialnego za utworzenie, usunięcie czy nadpisanie danych oraz czas tej operacji. 17) Ze względu na wymóg niskiego czasu dostępu do danych obszaru szybkiego system musi implementować protokół NFS over RDMA. 18) System musi mieć mechanizm deduplikacji danych celem optymalizacji wykorzystania przestrzeni dyskowych. 19) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Pozostałe wymagane funkcjonalności	1) Możliwość tworzenia lokalnych kopii migawkowych ręcznie lub automatycznie przy pomocy harmonogramu w którym definiuje się czas lub częstotliwość tworzenia kopii migawkowych oraz czas ich wygaśnięcia. Kopie migawkowe, których czas wygaśnięcia upłynął, powinny być automatycznie kasowane. Urządzenie powinno umożliwiać tworzenie kopii migawkowych z dokładnością do pojedynczego folderu. Mechanizm kopii migawkowych powinien się integrować z wykorzystywaną lub planowaną do wykorzystania w

	projekcie przez Zamawiającego usługą Microsoft Volume Shadowcopy, umożliwiając użytkownikowi końcowemu samodzielne odzyskanie danych (bez angażowania administratora systemu). 2) Rozwiązanie powinno umożliwiać tworzenie kopii migawkowych (ang. snapshot) również w trybie odczyt/zapis. 3) System powinien posiadać funkcjonalność WORM i powinien pozwalać na tworzenie zasobów (folderów/udziałów plikowych) zarówno objętych politykami WORM, jak i zasobów nie objętych taką polityką. Na jednym urządzeniu powinna być możliwość zdefiniowania zasobów objętych różnymi politykami WORM jednocześnie (np. różnym czasem retencji). Dla zasobów objętych funkcjonalnością WORM powinna istnieć możliwość obejścia polityki WORM poprzez uprzywilejowane kasowanie danych przez uprawnionego do tego użytkownika (np. root, czy tzw. Security Officer). Dla zasobów objętych polityką WORM powinna istnieć możliwość przedłużenia czasu retencji na potrzeby np. dochodzenia (tzw. Litigation Hold). System powinna pozwalać na ręczne ustawianie flagi WORM, jak i na automatyczne nakładanie retencji (np. po określonym czasie od utworzenia pliku) bez dodatkowej akcji ze strony aplikacji. 4) Razem z rozwiązaniem należy dostarczyć platformę umożliwiającą zarządzanie danymi (indeksowanie, przeszukiwanie, czy opisywanie danych – dodawanie tzw. „tag-ów") i raportowanie bazujące m. in na ww. „tag-ach". 5) Polityki warstwowego składowania danych (ang. tiering) muszą umożliwiać elastyczne definiowanie kryteriów przenoszenia plików pomiędzy poszczególnymi tier-ami bazując m. in. na czasie utworzenia pliku (ctime), ostatnim czasie dostępu do pliku (atime), ostatnim czasie modyfikacji pliku (mtime), wielkości pliku, lokalizacji pliku (ścieżce), rozszerzeniu pliku i nazwie pliku. 6) Replikacja zdalna również musi być definiowalna na poziomie wybranego katalogu/udziału. System musi wspierać replikację dwukierunkową, jeden-do-wiele i wiele-do-jeden (na poziomie całego systemu). W celu zapewnienia dodatkowych punktów odzyskiwania danych (ang. Point-in-Time) musi istnieć możliwość automatycznego tworzenie kopii migawkowych na zdalnej macierzy po zakończeniu procesu replikacji. 7) Rozwiązanie musi mieć możliwość rozbudowy o funkcjonalność tworzenia kopii zapasowych danych na nim składowanych przy pomocy protokołu NDMP w trybie „2-way-NDMP" (bezpośrednio po sieci SAN). Zamawiający nie wymagana dostarczenia tej funkcjonalność w ramach tego postępowania.

	8) Jeżeli system wymaga zewnętrznych komponentów zapewniających komunikację pomiędzy węzłami (np. w postaci przełączników), muszą one pochodzić od tego samego producenta co system i muszą być uwzględnione w ofercie. 9) Możliwość zabezpieczenia wybranych danych (np. poprzez ustawianie takiego parametru dla poszczególnych folderów) przed nieuprawnioną edycją lub skasowaniem za pomocą mechanizmu WORM. Polityki WORM powinny być replikowane do zdalnego systemu.

5. System archiwalnej pamięci masowej o dostępie plikowym

Zaoferowany system archiwalnej pamięci masowej o dostępie plikowym musi spełniać wszystkie wymagania przedstawione w poniższej tabeli.

Parametr	Charakterystyka (wymagania minimalne)
Pojemność, wydajność i bezpieczeństwo systemu	1) Zaoferowany system pamięci masowej o dostępie plikowym (zwanym dalej systemem) musi być zbudowany w architekturze „scale-out" (skalowalnej horyzontalnie). 2) System musi być zbudowany w oparciu jednakowe węzły serwerowe (kontrolerowo-dyskowe) zwane dalej węzłami. 3) Dostarczony system musi zapewnić pojemność użyteczną minimum 1800 TiB. Pojemność użyteczną należy rozumieć jako pojemność prezentowaną do serwerów i pozwalającą na rzeczywisty zapis danych o tej objętości na macierzy bez uwzględnienia mechanizmów redukcji danych. Pojemność użyteczna to pojemność po odliczeniu wszelkich narzutów związanych z organizacją danych na dyskach takich jak przechowywanie parzystości, sum kontrolnych, danych systemowych, pojemności zapasowej, itp. 4) Architektura systemu oraz zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 3 (trzech) dowolnych dysków jednocześnie lub jednego węzła (kontrolera). 5) Wymagane mechanizmy ochrony przed awarią dysku to RAID lub kodowanie nadmiarowe (ECC). 6) Rozwiązanie musi umożliwiać ochronę danych przy pomocy wielokrotnego zapisu (ang. mirroring). 7) Musi istnieć możliwość zmiany protekcji danych przy zachowaniu nieprzerwanej dostępności zasobów, również pomiędzy trybem ECC i mirroring, w tym również dla plików w obrębie tego samego folderu, bez konieczności ich przenoszenia na inny zasób. 8) System musi udostępniać całą dostępną przestrzeń w ramach jednego ciągłego systemu plików, który musi być skalowalny do co najmniej 20 PiB powierzchni użytecznej. 9) System musi zapewniać wydajność: a) wydajność nie mniejsza niż 85 MB/s (megabajtów na sekundę) w przypadku losowych odczytów protokołem NFS v.3 (RFC 1813) dla bloku o wielkości 4KB i nie więcej niż 30 jednoczesnych wątków (ang. threads) na węzeł, b) wydajność nie mniejszą niż 420 tys. file OPS (operacji plikowych na sekundę) w teście SPEC SFS 2014 dla obciążenia zdefiniowanego jako SWBUILD przy zachowaniu średnich opóźnień nie większych niż 9ms.

	Oferent musi przedstawić wyniki testu potwierdzające spełnienie tego warunku, potwierdzone przez producenta sprzętu. 10) System musi być zbudowany z 10 jednakowych węzłów (kontrolerów), gdzie każdy realizuje dostęp plikowy do danych i zapewnia wysoką wydajność dostępu do zgromadzonych plików w systemie. Dopuszcza się rozwiązanie, gdzie węzeł (kontroler) pełni jednocześnie rolę półki dyskowej. 11) System musi umożliwiać rozbudowę do co najmniej 200 węzłów w ramach tego samego systemu dyskowego, prezentujących do klientów jeden system plików. 12) System nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie: a) dysków b) interfejsów sieciowych c) kontrolerów (węzłów) d) zasilaczy e) wentylatorów.
Sprzęt	1) W celu maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, pojedynczy węzeł nie może zajmować więcej niż 1 RU w szafie. 2) System musi być dostarczony wraz z kompletem wszystkich niezbędnych elementów potrzebnych do połączenia poszczególnych węzłów w jeden system, zarządzany z jednego interfejsu administracyjnego. 3) Każdy węzeł musi być wyposażony w co najmniej 1 procesor klasy x86-64, z których każdy posiada minimum 16 rdzeni. 4) System musi zapewniać dostępną, łączną pojemność pamięci RAM nie mniejszą niż 3840 GB (tzn. min. 384 GB dla pojedynczego węzła). 5) Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci podręcznej (ang. cache) w oparciu o dyski SSD. 6) Każdy z elementów systemu musi być wyposażony w redundantne zasilacze zapewniające odporność na awarię pojedynczego źródła zasilania. 7) Każdy węzeł musi być wyposażony w 2 karty sieciowe Ethernet: a) jedna dwu-portowa karta 100 Gb/s Ethernet QSFP28 na potrzeby wewnętrznej komunikacji węzłów (interfejsy typu „back-end”) b) jedna dwu-portowa karta 100 Gb/s Ethernet QSFP28 przeznaczone do zapewniania dostęp do danych (interfejsy typu „front-end”).

	8) Każdy węzeł musi być wyposażony w: a) co najmniej 20 jednakowych dysków typu NLSAS lub SATA o pojemności co najmniej 12 TB każdy przeznaczonych do przechowywania danych b) co najmniej 2 jednakowe dyski SSD o pojemności minimum 3.2 TB każdy do buforowania metadanych i samych danych (ang. cache). 9) System musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu wszystkich interfejsów typu „front-end". 10) Komunikacja pomiędzy węzłami („back-end") musi: a) odbywać się za pośrednictwem osobnych i dedykowanych tylko do tego celu interfejsów (niewspółdzielonych z portami dostępowymi – „front-end"), b) odbywać się za pośrednictwem dedykowanych i przeznaczonych tylko do tego celu przełączników sieciowych (niewspółdzielonych z przełącznikami obsługującymi dostęp do danych – „front-end"), c) być zrealizowana w sposób redundantny, zapewniający prawidłową pracę systemu w przypadku awarii dowolnego przełącznika sieciowego obsługującego komunikację pomiędzy węzłami („back-end"). Wszystkie niezbędne elementy zapewniające tą komunikację (tj. przełączniki sieciowe, okablowanie, inne) muszą być dostarczone wraz z systemem i nie podlegają szczegółowej specyfikacji przez Zamawiającego. Zmawiający nie dopuszcza możliwość realizacji tych połączeń przy użyciu kabli typy „DAC" (ang. Direct Attach Cable). 11) System musi zapewnić gwarantowaną ochronę przed tzw. „cichym uszkodzeniem danych" (ang. silent data corruption) dla wszystkich technologii dyskowych. 12) System musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia dowolnego z elementów urządzenia. Musi posiadać zaimplementowany system jednoznacznego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej przy uszkodzonym dysku. 13) System musi zapewniać pracę jednocześnie wszystkich węzłów w trybie aktywny/aktywny w celu zapewnienia niezawodności i dostępności danych (tzn. każdy kontroler powinien umożliwiać dostęp do wszystkich danych oraz prezentować spójny widok systemu plików).
Funkcjonalność	1) System musi umożliwiać dynamiczne rozszerzanie i zmniejszanie udostępnianych systemów plików bez konieczności:

	a) modyfikacji już zainstalowanych węzłów, b) ręcznej migracji/dystrybucji danych na nowe dyski systemu. 2) System musi zapewniać dostęp z rożnych systemów operacyjnych (wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego: UNIX, macOS, Linux, Windows) z wykorzystaniem standardowych protokołów. Wymagana jest poprawna obsługa co najmniej: NFS v3 i v4, SMB (CIFS) v2 i v3, FTP, HTTP i S3 API. 3) System musi wspierać natywnie Hadoop Distributed File System (HDFS). 4) Jednoczesny dostęp do tych samych danych musi być możliwy przy wykorzystaniu wszystkich protokołów wymienionych powyżej. System musi również umożliwiać zarządzanie uprawnieniami użytkowników w dostępie wieloprotokołowym. 5) System musi zapewnić obsługę alertów i umożliwiać monitorowanie za pomocą protokołu SNMP (w wersji min. 2c). 6) System musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 7) System musi posiadać funkcjonalność asynchronicznej replikacji danych z wykorzystaniem protokołu TCP/IP celem dystrybucji treści i zapewnienia kopii danych w zdalnej lokalizacji. 8) System musi posiadać funkcjonalność wykonywania kopii migawkowych (ang. snapshot) oraz pozwalać stworzenie co najmniej 1000 kopii migawkowych dla danego katalogu w celu zapewnienia lokalnej ochrony danych. 9) System musi obsługiwać funkcjonalność realizacji kopii zapasowej (ang. backup) za pomocą protokołu NDMP. 10) System musi posiadać wbudowaną funkcjonalność definiowania limitów ilości danych (tzw. quoty) dla wybranych katalogów, użytkowników oraz grup użytkowników. 11) System musi posiadać mechanizm dystrybucji połączeń pomiędzy węzłami (ang. load-balancing) bez potrzeby stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. Load-balancing musi być dostępny i być wspierany zarówno dla protokołów plikowych, jak i dla obiektowych (S3 API). 12) Administracja systemem musi odbywać się poprzez interfejs graficzny dostępny przez przeglądarkę internetową (poprawna obsługa przez przeglądarki co najmniej Google Chrome i Mozilla Firefox) oraz wiersz poleceń (ang. Command Line Interface, CLI).

	Musi również istnieć możliwość zarządzania przy pomocy interfejsu programistycznego REST API. 13) Rozwiązanie musi udostępniać statystyki historyczne z wykorzystania systemu i zapewniać statystyki wykorzystania zasobów przez użytkowników oraz generowanie raportów graficznych, w tym raportów porównujących dostępne parametry systemu. 14) System musi posiadać funkcjonalność automatycznego „tiering-u", tzn. przesuwania danych w zależności od ich utylizacji pomiędzy warstwami dyskowymi (ang. tiers), w ramach jednego systemu plików i według polityk ustawionych przez administratora. Dostęp w trybie odczyt/zapis do danych musi być zachowany cały czas, również w trakcie operacji przenoszenia danych (ang. tiering), czy zmiany poziomu protekcji danych (np. z n+1 na n+2) (ang. re-striping). 15) System musi posiadać funkcjonalność monitorowania wydajności (obciążenie CPU lub interfejsów sieciowych, opóźnienia, ilość operacji na sekundę, wydajność per protokół itp.) oraz analityki systemu plików („capacity planning", zmiany na systemie plików). 16) System musi posiadać wbudowaną funkcjonalność audytu, która daje co najmniej możliwość precyzyjnego określenia użytkownika odpowiedzialnego za utworzenie, usunięcie czy nadpisanie danych oraz czas tej operacji. 17) Ze względu na wymóg niskiego czasu dostępu do danych obszaru szybkiego system musi implementować protokół NFS over RDMA. 18) System musi mieć mechanizm deduplikacji danych celem optymalizacji wykorzystania przestrzeni dyskowych. 19) Jeżeli do spełnienia któregokolwiek z wymagań zdefiniowanych powyżej wymagane jest dodatkowe oprogramowanie lub licencja - należy je dostarczyć wraz z zamawianym systemem w wersji bez ograniczeń czasowych na całą pojemność systemu.
Dodatkowe funkcjonalności	1) Możliwość tworzenia lokalnych kopii migawkowych ręcznie lub automatycznie przy pomocy harmonogramu w którym definiuje się czas lub częstotliwość tworzenia kopii migawkowych oraz czas ich wygaśnięcia. Kopie migawkowe, których czas wygaśnięcia upłynął, powinny być automatycznie kasowane. Urządzenie powinno umożliwiać tworzenie kopii migawkowych z dokładnością do pojedynczego folderu. Mechanizm kopii migawkowych powinien się integrować z wykorzystywaną lub planowaną do wykorzystania w projekcie przez Zamawiającego usługą Microsoft Volume Shadowcopy, umożliwiając użytkownikowi końcowemu samodzielne odzyskanie danych (bez angażowania administratora systemu).

	2) Rozwiązanie powinno umożliwiać tworzenie kopii migawkowych (ang. snapshot) również w trybie odczyt/zapis. 3) System powinien posiadać funkcjonalność WORM i powinien pozwalać na tworzenie zasobów (folderów/udziałów plikowych) zarówno objętych politykami WORM, jak i zasobów nie objętych taką polityką. Na jednym urządzeniu powinna być możliwość zdefiniowania zasobów objętych różnymi politykami WORM jednocześnie (np. różnym czasem retencji). Dla zasobów objętych funkcjonalnością WORM powinna istnieć możliwość obejścia polityki WORM poprzez uprzywilejowane kasowanie danych przez uprawnionego do tego użytkownika (np. root, czy tzw. Security Officer). Dla zasobów objętych polityką WORM powinna istnieć możliwość przedłużenia czasu retencji na potrzeby np. dochodzenia (tzw. Litigation Hold). System powinna pozwalać na ręczne ustawianie flagi WORM, jak i na automatyczne nakładanie retencji (np. po określonym czasie od utworzenia pliku) bez dodatkowej akcji ze strony aplikacji. 4) Razem z rozwiązaniem należy dostarczyć platformę umożliwiającą zarządzanie danymi (indeksowanie, przeszukiwanie, czy opisywanie danych – dodawanie tzw. „tag-ów") i raportowanie bazujące m. in na ww. „tag-ach". 5) Polityki warstwowego składowania danych (ang. tiering) muszą umożliwiać elastyczne definiowanie kryteriów przenoszenia plików pomiędzy poszczególnymi tier-ami bazując m. in. na czasie utworzenia pliku (ctime), ostatnim czasie dostępu do pliku (atime), ostatnim czasie modyfikacji pliku (mtime), wielkości pliku, lokalizacji pliku (ścieżce), rozszerzeniu pliku i nazwie pliku. 6) Replikacja zdalna również musi być definiowalna na poziomie wybranego katalogu/udziału. System musi wspierać replikację dwukierunkową, jeden-do-wiele i wiele-do-jeden (na poziomie całego systemu). W celu zapewnienia dodatkowych punktów odzyskiwania danych (ang. Point-in-Time) musi istnieć możliwość automatycznego tworzenie kopii migawkowych na zdalnej macierzy po zakończeniu procesu replikacji. 7) Rozwiązanie musi mieć możliwość rozbudowy o funkcjonalność tworzenia kopii zapasowych danych na nim składowanych przy pomocy protokołu NDMP w trybie „2-way-NDMP" (bezpośrednio po sieci SAN). Zamawiający nie wymagana dostarczenia tej funkcjonalność w ramach tego postępowania. 8) Jeżeli system wymaga zewnętrznych komponentów zapewniających komunikację pomiędzy węzłami (np. w postaci przełączników), muszą one pochodzić od tego samego producenta co system i muszą być uwzględnione w ofercie.

	9) Możliwość zabezpieczenia wybranych danych (np. poprzez ustawianie takiego parametru dla poszczególnych folderów) przed nieuprawnioną edycją lub skasowaniem za pomocą mechanizmu WORM. Polityki WORM powinny być replikowane do zdalnego systemu.

6. Oprogramowanie do wykonywania kopii zapasowych

Zaoferowane oprogramowanie do wykonywania kopii zapasowych musi spełniać wszystkie wymagania przedstawione poniżej.

1) Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do wykonywania kopii zapasowych (ang. backup) całego środowiska „data center" składającego się z maszyn wirtualnych.
2) Wymagane jest dostarczenie wszystkich modułów oprogramowania do wykonywania kopii zapasowych tak, aby zapewnić backup całości dostarczanego środowiska oraz spełnić wszystkie wymienione w poniżej funkcjonalności.
3) Wymagane jest by wszystkie dostępne funkcjonalności oferowanego oprogramowania do wykonywania kopii zapasowych były odblokowane w ramach oferowanej licencji procesorowej.
4) W szczególności wymagane jest by w ramach dostarczonej licencji była możliwość tworzenia kopii oraz odtwarzania:
   a) dowolnej liczby maszyn wirtualnych jako obrazów (ang. „image level")
   b) agentowo:
      i) dowolnej liczby baz danych,
      ii) dowolnej liczby plików – zarówno z serwerów niezwirtualizowanych jak również ze środka maszyn wirtualnych
   c) użycia dowolnej liczby mediów backupowych o dowolnej pojemności
5) Serwer kopii zapasowych musi być uruchomiony jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.
6) Wymagane jest by serwer backupu działał jako maszyna wirtualna na wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego systemie operacyjnym Windows / Linux.
7) Wymagane jest by serwer backupu, jako maszyna wirtualna, wspierał przenoszenie maszyny wirtualnej serwera backupu do innej lokalizacji mechanizmami wirtualizatora.
8) Serwer backupu nie może zużywać więcej zasobów niż:
   a) 2 procesory wirtualne 8 wątków każdy procesor
   b) 32 GB pamięci RAM
   c) 200 GB dysku
9) Oprogramowanie backupowe musi umożliwiać backup zabezpieczanych maszyn na oferowane medium de-duplikacyjne zarówno poprzez sieć LAN jak również SAN.
10) Wymagane jest by istniała możliwość wyboru miejsca de-duplikacji
    a) na źródle
    b) na medium backupowym
    zarówno dla backupu po LAN jak i SAN
11) Backup z de-deduplikacją na źródle musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych w każdym z przypadków:
    a) backup po LAN
    b) backup po SAN.

12) Oprogramowanie backupowe musi zapewniać backup z każdej zabezpieczanej maszyny bezpośrednio na zaoferowanym urządzeniu do przechowywania kopii zapasowych (medium de-duplikacyjne) bez pośrednictwa jakichkolwiek innych serwerów. Funkcjonalność musi dostępna dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego następujących systemów: Windows, RedHat, SuSE, Solaris.
13) Oprogramowanie backupowe musi zapewniać bezpośredni backup z de-duplikacją na źródle z każdej zabezpieczanej maszyny znajdującej się w sieci LAN bezpośrednio na oferowane medium de-duplikacyjne bez pośrednictwa jakichkolwiek innych serwerów. Funkcjonalność musi być dostępna dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego następujących systemów: Windows, RedHat, SuSE, Solaris.
14) W przypadku awarii połączenia LAN, oprogramowanie backupu musi mieć możliwość automatycznego przełączenia się na inną dostępną ścieżkę LAN i kontynuowania procesu backupu bez konieczności jakiejkolwiek interwencji administratora oraz bez wznawiania procesu backupu.
15) Wymagane jest by oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows / Linux.
    W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików. Jednocześnie musi być możliwość odtworzenia:
    a) całego wolumenu
    b) pojedynczego pliku.
    Celem minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje istotne wydłużenie czasu backupu).
16) Wymagane jest by oprogramowanie backupowe zapewniało pełny backup blokowy wielomilionowych systemów plików na maszynach Windows / Linux poprzez odczyt tylko zmienionych bloków.
    Wymagane jest by odczyt całości zabezpieczanego dysku był wykonywany tylko raz, podczas pierwszego backupu. Wszystkie kolejne backupy mają odczytywać z dysku tylko zmienione bloki od ostatniego backupu (przy czym na medium backupowym powinien być pełen backup).
    Dopuszcza się odczyt całości danych na dysku po restarcie serwera.
    Oprogramowanie backupowe nie może odczytywać zmienionych plików, jedynie zmienione bloki na dysku.
17) Oferowane rozwiązanie backupowe musi przechowywać całość własnych informacji (informacje o backupach, napędach taśmowych, mediach) w centralnym pojedynczym katalogu. Skopiowanie centralnego katalogu systemu backupu na inną maszynę musi pozwolić na uruchomienie serwera backupu identycznego z oryginalnym na drugiej maszynie. Proces klonowania centralnego katalogu może odbywać się przy wyłączonych procesach backupowych (zapewnienie spójności wewnętrznej bazy danych systemu backupowego).
18) Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.
19) Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki:
    a) urządzenia dyskowe

b) zaoferowane urządzenie de-duplikacyjne
c) taśmy.

20) W przypadku backupu na nośniki taśmowe musi być możliwość zdefiniowania puli taśm (zawierającej jedną lub więcej taśm) na którą będą zapisywane tylko i wyłącznie backupy wewnętrznej bazy danych systemu backupowego.
21) Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych.
22) Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi mailowo raportować miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego.
23) Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego.
24) Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN i bezpośredni zapis na napędzie taśmowym (multiplexing). Proces multiplexingu nie może wymagać zapisu danych na dysk: czasowego czy tez trwałego.
25) Oprogramowanie backupowe musi umożliwiać zarządzanie replikacją backupów między kilkoma urządzeniami de-duplikacyjnymi (zaoferowanych w tym postępowaniu) bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań
    a) replikacji podlegają tylko te bloki które nie znajdują się na docelowym oferowanym urządzeniu de-duplikacyjnym
    b) replikacja między oferowanymi urządzeniami de-duplikacyjnymi może nastąpić zarówno bezpośrednio po zakończeniu backupu jak również zgodnie z harmonogramem
    c) oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się na urządzeniach de-duplikacyjnych.

    W trakcie odtwarzania, z graficznego GUI, oferowane oprogramowanie backupowe misi pozwalać na wybór urządzenia de-duplikacyjnego z którego zostanie wykonane odtwarzanie.
26) Rozwiązanie backupowe musi wspierać bezpośredni backup (bez użycia serwerów pośredniczących) z zabezpieczanych maszyn na macierz obiektową przy użyciu S3 API.
27) Wymagane jest by oferowane oprogramowanie backupowe wspierało backup na fizyczne macierze obiektowe przy użyciu S3 API.
28) Wymagane jest by backup na macierze obiektowe odbywał się:
    a) z de-duplikacją zmiennym blokiem
    b) z de-duplikacja na źródle
    c) poprzez transfer danych bezpośrednio z zabezpieczanych maszyn do macierzy obiektowej bez jakichkolwiek serwerów/elementów pośredniczących.

    Oznacza to, że agent oprogramowania backupowego musi dzielić zabezpieczane dane na kawałki zmiennej długości. Z zabezpieczanej maszyny bezpośrednio do macierzy obiektowej musza być przesłane tylko te kawałki danych, które się tam jeszcze nie znajdują. Funkcjonalność ta musi być dostępna dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego zabezpieczanych systemów Windows/Linux.
29) Wymagana jest funkcjonalność replikacji backupów wykonanych na macierz obiektową do:
    a) innej, dowolnie wspieranej macierzy obiektowej

b) biblioteki taśmowej (w postaci backupu bez deduplikacji, czyli w postaci takiej jak wykonanie oryginalnego backupu na bibliotekę taśmową)
c) zasobu dyskowego (w postaci backupu bez deduplikacji, czyli w postaci takiej jak wykonanie oryginalnego backupu na dysk).

30) Oprogramowanie backupowe musi mieć możliwość klonowania zadań backupowych między dowolnym mediami, minimum:
a) de-duplikacyjnymi
b) dyskowymi (CIFS, NFS)
c) taśmowymi
d) obiektowymi (S3).
31) Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replika backupu). Definicja czasu przechowywania kopii (repliki) musi być możliwa w momencie definiowania zadania duplikacji / klonowania zarówno z interfejsu graficznego jak i z wiersza poleceń (ang. Command Line Interface, CLI).
32) Oprogramowanie backupowe musi wspierać multiplexing w procesie klonowania / duplikacja danych na nośniki taśmowe.
Oznacza to, że w przypadku jednoczesnego klonowania/duplikacji 20 zadań backupowych z de-duplikatora na pojedynczy napęd taśmowy, wszystkie 20 klonowane/duplikowane zadania musi być jednocześnie w tym samym czasie zapisywane na pojedynczy napęd taśmowy.
33) Oprogramowanie backupowe musi pozwalać na backup systemu plików:
a) pełny
b) różnicowy
c) inkrementalny.
34) Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełny backup. Proces ten musi być niewidoczny dla systemu plików którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w kontekście zarówno:
a) zarządzania
b) wydajności.
35) Łączenie backupów pełnych i inkrementalnych musi odbywać się przez oferowane urządzenie de-duplikacyjne. Jedynie zarządzenie (start, kalendarz łączenia) procesem łączenia backupów pełnych i inkrementalnych musi odbywać się przez aplikację backupową.
36) Oferowane rozwiązanie backupowe musi pozwalać na wymuszenie blokady skasowania backupów na oferowanym urządzenie de-duplikacyjnym. Na przykład blokada skasowania backupu przez 15 dni oznacza, że:
a) Przez 15 dni nikt (również żaden z administratorów) nie może usunąć backupu
b) Przez 15 dni nikt (również żaden z administratorów) nie może zmienić backupu
c) Przez 15 dni nikt (również żaden z administratorów) nie może zmienić czasu blokady backupu
37) Blokada przed skasowaniem backupu musi być bezwzględna (ang. compliance). Nie może być możliwości cofnięcia blokady jakimikolwiek metodami.
38) Blokada backupu musi rozpocząć się bezpośrednio po zakończeniu wykonywania tego backupu.
39) Blokada backupu musi być możliwa do ustawienia dla każdego zadania backupowego, musi być możliwość ustawienia innego czasu blokady dla różnych zadań backupu.

40) Blokada backupu musi być możliwa dla minimum wszystkich następujący backupów:
    a) backup plikowy z wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego systemów: Linux / Windows / Unix
    b) backup obrazów maszyn wirtualnych z zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej
    c) backup wspieranych baz danych.
41) Oprogramowanie backupowe musi pozwalać na zatrzymanie procesu backupu oraz jego wznowienie od momentu zatrzymania.
42) W przypadku nieudanego backupu dla systemu plików (na przykład zerwanie łącza), oprogramowanie backupowe musi pozwalać na wznowienie backupu od ostatnio poprawnie zbackupowanego:
    a) katalogu
    b) pliku.
43) W przypadku awarii fragmentu taśmy, oprogramowanie backupowe musi odtworzyć całość plików, które znajdują się na nieuszkodzonej części nośnika.
44) W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usuwane.
45) Oprogramowanie musi umożliwiać kopię zapasową:
    a) pojedynczych plików
    b) całych systemów plików
    c) baz danych w trakcie ich normalnej pracy
    d) ustawień wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego systemu operacyjnego Windows
    e) całych obrazów maszyn wirtualnych systemu z zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.
46) Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) wykorzystywane lub planowane do wykorzystania w projekcie przez Zamawiającego następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Oracle Linux, CentOS), Solaris.
47) Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego aplikacji i baz danych: MS Exchange, MSSQL, Oracle, Oracle MySQL, PostgreSQL, MongoDB.
48) W przypadku baz danych system musi mieć wbudowaną możliwość inicjalizacji backupu określonym zdarzeniem: np. ilością logów, czasem który upłynął od ostatniego zdarzenia lub innym zdarzeniem zdefiniowanym przez użytkownika.
49) Dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego baz danych MSSQL musi być możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:
    a) backup jest wykonywany przez oferowane oprogramowanie backupowe
    b) inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio
    c) możliwość wyboru backupu pełnego, różnicowego

d) backup inicjowany przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego.

50) Dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego baz danych MSSQL musi być możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań:
   a) odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe
   b) zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio
   c) możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL
   d) odtworzenie bazy danych przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego.
51) Oferowane rozwiązanie backupowe musi integrować się funkcjonalnością FRA (Fast Recovery Area) wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego baz danych Oracle. Musza być spełnione wszystkie poniższe funkcjonalności:
   a) administrator Oracle wykonuje backupy narzędziami RMAN do przestrzeni FRA
   b) oferowane rozwiązanie backupowe automatycznie kopiuje backupy z przestrzeni Oracle FRA na media zarządzane przez oferowane rozwiązanie backupowe.
   c) definiowanie parametrów zadania kopiowania backupów przestrzeni FRA na media zarządzane przez oferowane rozwiązanie backupowe z poziomu interfejsu graficznego
   d) odtworzenie danych możliwe przez administratora Oracle bez kontaktu z administratorem oprogramowania backupowego
   e) w procesie odtwarzania, administrator Oracle nie musi wskazywać miejsca, gdzie znajdują się odtwarzane dane (przestrzeń FRA, media oferowanego rozwiązania backupowego).
52) Oprogramowanie backupowe musi być zarządzane z jednego miejsca poprzez jedną centralną konsolę zarządzającą
53) Konsola oprogramowania backupowego musi umożliwiać definiowanie polityk backupowych obejmujących całość cyklu życia kopii zapasowej.
   W szczególności musi być możliwość zdefiniowania polityki backupowej, która dla dowolnej liczby zabezpieczanych systemów (zadań backupowych) wymusza:
   a) lokalny backup na oferowane medium de-duplikacyjne z retencją miesięczną
   b) replikę zmian do medium de-duplikacyjnego w zdalnej lokalizacji (retencja 60 dni) replikacja odbywa się między urządzeniami de-duplikacyjnymi
   c) replikacja backupu z lokalnego medium de-duplikacyjnego na medium taśmowe (retencja 5 lat)
   d) replikacja backupu ze zdalnego medium de-duplikacyjnego na medium obiektowe (S3).
   Całość powyższych operacji musi być możliwa do zdefiniowania jako pojedyncza polityka backupowa definiowana z poziomu interfejsu graficznego oprogramowania backupowego przy pomocy kreatora (ang. wizard).
   Polityka musi mieć możliwość uruchomienia dla dowolnej liczby serwerów / zadań backupowych.
   Operacje opisane w a) do c) (duplikaty / klony) muszą mieć możliwość zdefiniowania opóźnienia rozpoczęcia wykonywania celem wykonania ich po oknie backupowym (duplikaty / klony nie obciążają wówczas mediów backupowych w trackie okna backupowego).

Administrator backupu musi mieć możliwość z poziomu interfejsu graficznego głównej konsoli oprogramowania backupowego odtworzenia dowolnej danych z dowolnych z powyższych kopii (1-4).

54) Rozwiązanie backupowe musi mieć możliwość odtworzenia plików na docelową maszynę z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę celem odtworzenia danych z systemu backupowego.
55) Musi istnieć możliwość odtworzenia danych z:
    a) zabezpieczanego serwera / komputera
    b) konsoli systemu backupowego.
56) Dla zaoferowanego środowiska wirtualizacji mocy obliczeniowej oprogramowanie backupowe musi umożliwiać następujące typy backupu:
    a) backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej
    b) backup całych maszyn wirtualnych (obrazów, plików reprezentujących wirtualną maszynę). W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn
    c) backup tylko wybranych dysków maszyny wirtualnej (wybranych plików systemu do wirtualizacji)
    d) w trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn
    e) Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane do medium backupowego przy pomocy technologii transferującej tylko zmienione bloki. Jednocześnie z punktu widzenia systemu backupowego musza to być backupy pełne. To znaczy z punktu widzenia systemu backupu muszą to być backupy identyczne z wykonywanym od zera pełnym backupem.
    f) Wykonywanie backupu jak w punkcie b. i c. nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych.

    Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium de-dupikacyjnego zgodnie z wymaganiami dla de-duplikacji powyżej.

    Powyższe metody backupu muszą być wbudowane w system backupu i być w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
57) Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych dostarczając następujące funkcjonalności:
    a) odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm w którym odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu
    b) odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm w którym odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu
    c) odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.

Powyższe metody odtworzenia muszą być wbudowane w system backupu i być w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

58) Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z medium backupowego bez konieczności odtwarzania (ang. Instant Access).
59) Z pojedynczego backupu maszyny wirtualnej musi być możliwość jednoczesnej realizacji wszystkich poniższych funkcjonalności:
    a) odtworzenie całej maszyny wirtualnej
    b) odtworzenie pojedynczego dysku maszyny wirtualnej
    c) odtworzenie pojedynczego pliku maszyny wirtualnej
    d) uruchomienie maszyny wirtualnej bez odtwarzania (ang. Instant Access).
60) Skalowalność rozwiązania dla środowiska wirtualizacyjnego musi pozwalać na:
    a) backup minimum 5000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu
    b) pełny backup minimum 1000 maszyn wirtualnych backupowanych w ciągu godziny w ramach pojedynczej instancji systemu backupu.
61) Rozwiązanie backupowe musi umożliwiać backup i odtwarzanie równolegle, w tym samym czasie minimum 100 maszyn wirtualnych. Wykonywane równoległe backupy maszyn wirtualnych musza być backupami pełnymi przy odczycie tylko zmienionych bloków.
62) Rozwiązanie backupowe musi umożliwiać backup minimum 25 maszyn wirtualnych z pojedynczego serwera proxy (z pojedynczego serwera odczytującego obrazy maszyn wirtualnych). Wszystkie 25 sesji backupujących wirtualne maszyny musi odczytywać tylko zmienione bloki wykonując przy tym pełny backup.
63) Rozwiązanie backupowe musi pozwalać na podłączenie do wielu instancji oprogramowania do zarządzania klastrem wirtualizacyjnym.
64) Rozwiązanie backupowe musi pozwalać na odtworzenie maszyny wirtualnej pomiędzy różnymi instancjami oprogramowania do zarządzania klastrem wirtualizacyjnym zdefiniowanymi w oprogramowaniu backupowym. Z poziomu interfejsu graficznego oprogramowania backupowego, w kreatorze odtwarzania, musi być możliwość wyboru maszyny wirtualnej znajdującej się w jednej instancji i możliwość wyboru innej instancji do którego maszyna wirtualna jest odtwarzana.
65) Administrator aplikacji backupowej musi mieć możliwość odtworzenia maszyny wirtualnej z GUI (graficzna konsola) dla każdego z poniższych sposobów:
    a) odtworzenie całej maszyny wirtualnej
    b) odtworzenie pojedynczego dysku z wcześniej zrobionej kopii całej maszyny wirtualnej
    c) odtworzenie plików / katalogów z backupu obrazów maszyny wirtualnej
    d) uruchomienie maszyny wirtualnej z medium backupowego bez odtwarzania
    e) naprawienie maszyny wirtualnej na obecnej instancji – odtworzenie tylko zmienionych bloków od ostatniego backupu.

    Wszystkie powyższe możliwości muszą być dostępne w postaci graficznych kreatorów.
66) Administrator (właściciel) danej maszyny wirtualnej musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem środowiska wirtualizacyjnego) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej z poziomu interfejsu graficznego dostępnego ze środka maszyny wirtualnej – dostarczanego przez oprogramowanie backupowe.

67) Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych dla każdej wykonanej w przeszłości kopii zapasowej.
Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
68) Rozwiązanie backupowe musi pozwalać na automatyczne polityki backupowe dla np. folderu. Oznacza to, że dodanie maszyny wirtualnej do folderu spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu.
69) Wymagane jest by w środowisku wirtualizacyjnym oprogramowanie backupowe pozwalało na automatyczne dodawanie maszyn wirtualnych do odpowiednich polityk na podstawie każdej z poniższych możliwości:
    a) automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych zawierających w nazwie maszyny wirtualnej podany tekst
    b) automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się we wszystkich folderach zawierających w nazwie podany tekst
    c) automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych których tag zawiera podany tekst.

    Automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się na wszystkich magazynach danych które w nazwie zawierają podany tekst.
70) Oprogramowanie backupowe musi automatycznie rozpoznawać nowe, utworzone maszyny wirtualne i umieszczać je w odpowiednich politykach backupowych. Wymagana jest możliwość konfiguracji poniższego scenariusza:
    a) wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowane automatycznie co godzinę
    b) wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowane automatycznie raz na dzień
    c) pozostałe maszyny wirtualne mają być backupowane raz na tydzień

    Powyższe rozwiązanie backupowe musi wykonywać się samoczynnie, bez jakichkolwiek akcji ze strony administratora backupu, administratora środowiska wirtualizacyjnego czy też jakiekolwiek innej osoby.
71) Wymagane jest by oprogramowanie backupowe pozwalało na automatyczne usuwanie maszyn wirtualnych z polityk backupowych w tym samym momencie, w którym maszyna jest usunięta z środowiska wirtualizacyjnego.
Jednocześnie dotychczasowo wykonane kopie zapasowe muszą być przechowywane zgodnie z retencją celem możliwości odtworzenia uśniętej wcześniej maszyny wirtualnej.
72) Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu wirtualizacyjnego z poziomu instancji oprogramowania do zarządzania klastrem wirtualizacyjnym. Administrator ten musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.
73) Całość informacji o backupach środowiska wirtualizowanego musi być przechowywana centralnie, na serwerze backupu.
74) Maszyna wirtualna zbackupowana przez serwer pośredniczący, musi mieć możliwość odtworzenia przez dowolny inny serwer pośredniczący.
75) Oprogramowanie backupowe musi samo dystrybuować zadania backupu/odtwarzania obrazów maszyn wirtualnych pomiędzy dostępne serwery pośredniczące.

7. Oprogramowanie do wirtualizacji

Zaoferowane oprogramowanie do wirtualizacji musi być w pełni kompatybilne ze sobą w ramach wszystkich zaoferowanych modułów, których specyfikację zawarto w poniższych podpunktach.

7.1. Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji

1) Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. Software-Defined Networking).
2) Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania opisane w tym rozdziale musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.

7.2. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej

1) Zaoferowane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej musi:
   a) być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego
   b) alokować dla własnych celów nie więcej niż 600MB pamięci operacyjnej RAM serwera fizycznego
   c) potrafić obsłużyć i wykorzystać zasoby fizyczne serwera: 2 procesory fizyczne, co najmniej 128 logicznych wątków procesora, 2TB pamięci fizycznej RAM
   d) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do minimum 256 procesorów wirtualnych
   e) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia minimum 4 TB pamięci operacyjnej RAM
   f) zapewniać możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej
   g) zapewniać możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
   h) wspierać następujące wykorzystywane lub planowane do wykorzystania w projekcie przez Zamawiającego systemy operacyjne: Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 12, SLES 11, RHEL 8, REHL 7, Solaris 11, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux
   i) umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są umieszczone
   j) umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych
   k) zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności co najmniej dla wykorzystywanego

lub planowanego do wykorzystania w projekcie przez Zamawiającego wirtualizatora (ang. hypervisor) Microsoft Hyper-V pakietu Microsoft Windows Server 2016 i nowszego na maszynie wirtualnej

l) umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych
m) 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 administratora („root")
n) zapewniać możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi
o) zapewniać możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością zachowania stanu pamięci pracującej maszyny wirtualnej
p) zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
q) posiadać funkcjonalność tworzenia wirtualnego przełącznika (ang. virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze serwera wirtualizacyjnego (ang. hypervisor) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego serwera, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 wirtualnych portów Ethernet
r) w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej pojedynczy wirtualny przełącznik, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych
s) posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN) na wirtualnych przełącznikach w zaoferowanym oprogramowaniu
t) zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
u) umożliwiać wykorzystanie technologii przepustowości sieci komputerowych 200 GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
v) obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
w) zapewniać możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
x) 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. Replikacja musi gwarantować współczynnik RPO (ang. Recovery Point Objective) na poziomie minimum 5 minut
y) obsługiwać przełączenie ścieżek używanych przy dostępie do pamięci masowej bez utraty komunikacji w przypadku awarii jednej ze ścieżek
z) mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia

natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi

aa) umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z serwerów wirtualizacyjnych na kolejnym działającym w tym samym klastrze serwerze (funkcjonalność wysokiej dostępności, ang. High Availability, HA)

bb) w środowisku z minimum dwoma serwerami wirtualizacyjnymi musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwera wirtualizacyjnego, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną

cc) zapewniać możliwość obsługiwania dysków wirtualnych maszyn do rozmiaru co najmniej 60 TB

dd) posiadać funkcjonalność zarządzania poprzez ustandaryzowany interfejs programistyczny (API)

ee) posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej

ff) być kompatybilne z TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że serwer wirtualizacyjny (ang. hypervisor) uruchomił się w niezmienionej formie

gg) posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego Microsoft Windows 10, Microsoft Windows 2016 i nowszych. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10, Microsoft Windows 2016 i nowszym wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane, np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana

hh) posiadać funkcjonalność szybkiego uruchamiania oprogramowania wirtualizacyjnego po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji oprogramowania, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego

ii) wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol) i NTP (ang. Network Time Protocol)

jj) posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych, w ramach klastra serwerów, w celu zwiększenia bezpieczeństwa dostępu warstwy wirtualizacji

kk) mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany

ll) zapewniać podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa

mm) 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

nn) posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym oprogramowaniem wirtualizacyjnym oraz z serwerem zarządzającym tym oprogramowaniem, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.

7.3. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej

1) Zaoferowane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej musi spełniać wszystkie wymagania z wersji podstawowej (opisanej w punkcie **7.2**).
2) Zaoferowane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej dodatkowo musi:
   a) umożliwiać automatyczne równoważenie obciążenia procesora i pamięci operacyjnej serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej
   b) zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizacyjnego (ang. hypervisor), a następnie wymuszać ten profil/konfigurację na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
   c) w środowisku z minimalnie dwoma serwerami wirtualizacyjnym, w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, oprogramowanie musi posiadać możliwość automatycznego bezprzerwowego przeniesienia działających maszyn wirtualnych na inny serwer wirtualizacyjny, który nie jest objęty aktualizacją, przed rozpoczęciem samej aktualizacji
   d) umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne. Przełącznik taki musi:
      i) 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
      ii) współpracować z protokołem NetFlow
      iii) umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port
      iv) 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
   e) mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych

f) w środowisku z minimum dwoma serwerami wirtualizacyjnymi, zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o minimalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwera wirtualizacyjnego, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną
g) mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
h) umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowanego wirtualnego urządzenia dedykowanego dla poszczególnych maszyn wirtualnych
i) 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
j) wspierać technologię rozproszonego udostępniania wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego procesora graficznego Nvidia Grid vGPU zainstalowanego w serwerze fizycznym do maszyn wirtualnych
k) wspierać funkcjonalność trwałej, nieulotnej pamięci (ang. Persistent Memory)
l) posiadać certyfikację dla wykorzystywanego lub planowanego do wykorzystania w projekcie przez Zamawiającego pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji sztucznej inteligencji (AI) i systemów (ang. framework) przeznaczonych dla kompleksowego rozwiązania AI
m) mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
n) umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image
o) wspierać protokół Remote Direct Memory Access (RDMA) poprzez konwergentny Ethernet – RoCE w wersji „v2", Fiber Channel over Ethernet (FCoE) i iSCSI rozszerzenie dla RDMA (iSER). Wymaga się aby maszyny wirtualne można było konfigurować z wykorzystaniem protokołu RDMA

7.4. Oprogramowanie do zarządzania klastrem wirtualizacyjnym

1) Zaoferowane oprogramowanie do zarządzania musi:
   a) posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności – zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się aby powyższa maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. virtual appliance. Instalacja ww. virtual appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych. Virtual appliance musi być uruchomiony za pomocą dostarczonego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej (zwanym dalej „wirtualizatorem")

b) posiadać wbudowany serwer zapory sieciowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz maszynami wirtualnymi na nich uruchomionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów
c) mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o wykorzystywane lub planowane do wykorzystania w projekcie przez Zamawiającego : domenę Microsoft Active Directory i Open LDAP
d) posiadać konsole graficzną, która musi być dostępna poprzez przeglądarkę internetową (co najmniej przez Google Chrome i Mozilla Firefox) i być wykonana z wykorzystaniem języka HTML5
e) posiadać funkcjonalność zcentralizowanego zarządzania hostami opartymi na rozwiązaniu dostarczanego wirtualizatora
f) posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby mechanizm kopii zapasowych wspierał protokoły: FTPS, HTTPS, SCP, FTP oraz http
g) posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia takich zasobów jak vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny musi być wykonany w standardzie HTML5
h) posiadać możliwość konfiguracji dostarczonego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej poprzez użycie schematów konfiguracji i umożliwiać załadowanie takiego schematu dla wielu serwerów równocześnie
i) umożliwiać jednoczesną aktualizację oprogramowania na wielu dostarczanych wirtualizatorach
j) zapewniać natywne mechanizmy wysokiej dostępności (ang. High Availability, HA) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną
k) w przypadku zarządzania serwerami opartymi o dostarczany wirtualizator zasobów serwerowych i ich mocy obliczeniowej, musi prezentować poziom zbalansowania obciążenia w klastrze opartym o ww. wirtualizatory
l) umożliwiać dostęp przez przeglądarkę do konsoli graficznej w sposób skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

7.5. Oprogramowanie do wirtualizacji sieci w wersji podstawowej

1) Zaoferowane oprogramowanie do wirtualizacji sieci w wersji podstawowej musi:
   a) oferować możliwość budowy sieci komunikacyjnych z wykorzystaniem protokołu IP w oparciu o środowiska wirtualne zintegrowane z zaoferowanym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej
   b) zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci protokołów sieciowych

c) posiadać funkcję tworzenia rozproszonego, wirtualnego przełącznika instalowanego bezpośrednio w zaoferowanym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej (ang. hypervisor), umożliwiającego tworzenie logicznych segmentów sieci w warstwie drugiej modelu ISO/OSI
d) posiadać funkcję tworzenia rozproszonego, wirtualnego routera instalowanego bezpośrednio w zaoferowanym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej (ang. hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska serwerów wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów w warstwie sieci modelu ISO/OSI musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników (poza środowisko wirtualizacyjne)
e) posiadać możliwość kreowania segmentów sieci wirtualnej przy użyciu technologii VxLAN i/lub GENEVE (ang. Generic Network Virtualization Encapsulation)
f) zapewnić funkcjonalność łączenia (ang. bridging) środowiska zwirtualizowanego opartego o technologię VxLAN/GENEVE z środowiskiem niezwirtualizowanym zdefiniowanego za pomocą technologii VLAN
g) zapewniać funkcjonalność wirtualnego routera wspierającego protokół routingu BGP
h) zapewniać funkcjonalność łączenia segmentów sieci w warstwie drugiej VLAN i GENEVE poprzez zastosowanie wirtualnej bramy
i) zapewniać funkcjonalność translowania adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego do środowiska wirtualnego (DNAT)
j) posiadać funkcjonalność serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zwirtualizowanego
k) posiadać interfejs programistyczny (API) umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji sieci wirtualnych
l) umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia poprawności działania systemu przed i po aktualizacji
m) zapewniać bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego maszyny wirtualnej jak również dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych urządzeń w warstwie L2-L4 modelu ISO/OSI na zewnątrz (poza warstwę wirtualizacji mocy obliczeniowej)
n) posiadać funkcjonalność rozproszonej, stanowej zapory sieciowej (ang. firewall), realizowanej bezpośrednio na poziomie wirtualnego interfejsu sieciowego maszyny wirtualnej, umożliwiającej tworzenie polityk bezpieczeństwa w warstwach L2-L4 modelu ISO/OSI. Zapora ta musi umożliwiać definiowanie reguł do warstwy L7 modelu ISO/OSI dla wybranych aplikacji, w celu zapewnienia kontroli przepływu danych oraz planowania mikrosegmentacji
o) zapewniać możliwość tworzenia reguł firewall w trybie bezstanowym dla różnych grup wirtualnych serwerów
p) zapewniać możliwość tworzenia reguł polityk bezpieczeństwa z wykorzystaniem parametrów takich jak adres IP, porty i protokoły, dodatkowe parametry obiektów, tj. nazwa maszyny wirtualnej, nazwa przełącznika wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny

q) zabezpieczać środowisko wirtualne przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny, poprzez zablokowanie ruchu z i do tej wirtualnej maszyny po zmianie jej adresu IP w sposób nieautoryzowany
r) posiadać możliwość zestawienia tuneli „IPsec Site-to-Site" z uwierzytelnieniem za pomocą współdzielonego klucza (ang. pre-shared key) lub certyfikatu.

7.6. Oprogramowanie do wirtualizacji sieci w wersji rozszerzonej

1) Zaoferowane oprogramowanie do wirtualizacji sieci w wersji rozszerzonej musi spełniać wszystkie wymagania z wersji podstawowej (opisanej w punkcie **7.5**).
2) Zaoferowane oprogramowanie do wirtualizacji sieci w wersji rozszerzonej dodatkowo musi:
   a) zapewniać funkcjonalności rozkładania i równoważenia ruchu (ang. Load-Balancing) pracującej w warstwach 4 do 7 modelu ISO/OSI. Funkcjonalność musi zapewniać następujące mechanizmy utrzymywania sesji (ang. SessionPersistent), minimum : adres źródłowy, cookie
   b) umożliwiać natywną integrację z minimum dwoma produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall w warstwie siódmej modelu ISO/OSI, w celu dodatkowej filtracji i inspekcji ruchu
   c) umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania klasy antywirus / antymalware w postaci bezagentowej. Poprzez bezagentowość zamawiający rozumie instalacje na poziomie wirtualizatora (hypervisora) serwerów, bez ingerencji w maszynę wirtualną
   d) posiadać funkcję łączenia segmentów sieci w warstwie drugiej modelu ISO/OSI (ang. bridge) dla VLAN i VXLAN poprzez zastosowanie fizycznego przełącznika
   e) posiadać możliwość tworzenia reguł bezpieczeństwa uwzględniających nazwy użytkowników, poprzez integrację z wykorzystywaną lub planowaną do wykorzystania w projekcie przez Zamawiającego Microsoft Active Directory z obsługą selektywnej synchronizacji
   f) posiadać funkcjonalność identyfikacji wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego typu aplikacji co najmniej MySQL, MS Active Directory, HTTP, DNS, DHCP, TLS na poziomie sieciowym modelu ISO/OSI w warstwach 5 - 7, a następnie móc wykorzystać wynik identyfikacji w rozproszonym, wewnętrznym firewall w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji
   g) w ramach inspekcji warstwy 7 modelu ISO/OSI, mieć funkcjonalność równoważenia ruchu (ang. Load Balancer) oraz oferować funkcję blokowania i modyfikacji URL
   h) w przypadku rozwiązania równoważenia ruchu (ang. Load Balancer) musi:
      i) posiadać możliwość dodawania do nagłówka znacznika XFF (X-Fowarder-For)
      ii) być zarządzana oraz instalowana w ramach jednego interfejsu graficznego (pojedynczej konsoli) w ramach zaoferowanego oprogramowania
   i) pozwalać na realizację równoważenia obciążenia (ang. Load balancing) w formie scentralizowanej, to znaczy poprzez instalację i procesowanie ruchu na dedykowanym komponencie - na serwerze fizycznym (bare metal) lub maszynie wirtualnej

j) posiadać funkcjonalność typu Identity Firewall umożliwiające obsługę sesji użytkowników na pulpitach wirtualnych (VDI) oraz serwerach aplikacji (RDSH) współdzielących pojedynczy adres IP
k) umożliwiać włączenie funkcjonalności rozproszonego Systemu Wykrywania Włamań (ang. Intrusion Detection System) za pomocą licencji instalowanych na serwerach wirtualizacyjnych i umożliwiającego realizację wykrywania włamań za pomocą dedykowanych sygnatur ataków
l) musi posiadać funkcjonalność wsparcia mechanizmu VRF w obrębie wirtualizacji sieci.

7.7. Oprogramowanie do automatyzacji zadań w ramach środowiska zwirtualizowanego

1) Zaoferowane oprogramowanie do automatyzacji zadań w ramach środowiska zwirtualizowanego musi:

a) posiadać portal typu „Self-Service" do automatycznego tworzenia i uruchamiania:
   i. wirtualnych systemów operacyjnych
   ii. platform aplikacyjnych
   iii. całych zestawów/systemów maszyn wirtualnych
b) posiadać interfejs graficzny Ul (ang. user interface), który:
   i. musi być dostępny poprzez przeglądarkę internetową
   ii. musi być wykonany w technologii opartej o HTML5
   iii. mieć możliwość katalogowania widoku poszczególnych typów usług według własnego wzorca
c) posiadać możliwość modyfikacji właściwości obiektów w katalogu (w tym co najmniej konfiguracji wirtualnego zasobu: ilość CPU, pamięć RAM, przestrzeń dyskowa, sieć), zarówno przed „provisioningiem" usługi jak i po „provisioningu"
d) za pomocą dodatkowej integracji, oferować w ramach katalogu usług informacje o kosztach danej usługi – modyfikowana na bieżąco w zależności od konfiguracji wirtualnego sprzętu (np. ilość instancji, ilość pamięci RAM, ilość CPU)
e) prezentować informacje w postaci wykresów o kluczowych metrykach maszyny wirtualnej, wytworzonej w ramach ustalonego procesu co najmniej takich jak CPU, pamięć RAM, liczbę operacji wejścia/wyjścia (IOPS), sieć
f) umożliwiać modyfikację wirtualnego sprzętu przypisanego do obiektu po "provisioningu" danego obiektu z katalogu
g) posiadać zestaw wbudowanych procesów/czynności automatyzacji dostarczania usług wraz z możliwością ich edycji oraz możliwość zmiany konfiguracji i tworzenia nowych kroków w procesie cyklu życia konkretnej usługi
h) informować o statusie usługi w czasie rzeczywistym, wymagane statusy to co najmniej: usługa zaakceptowana, zakolejkowana, odrzucona, w trakcie akceptacji. Dodatkowo zaoferowane oprogramowanie musi mieć możliwość wysłania informacji poprzez pocztę elektroniczną o zmianie statusu usługi
i) posiadać możliwość definiowania sieci wirtualnych, które łączą maszyny wirtualne w ramach zarządzanej platformy – rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN
j) posiadać możliwość definiowania sieci wewnętrznych jak i sieci zewnętrznych połączonych do sieci fizycznej pozwalającej na komunikację np. do Internetu za pomocą NAT –

rozwiązanie musi wspierać natywnie nie mniej niż dwa rozwiązania typu SDN, posiadać możliwość definiowania fizycznych zasobów (mocy obliczeniowej) oraz zmiany ich wielkości poprzez powiększenie lub pomniejszenie obiektu) bez wpływu na działanie usług – tj. obiekt musi być dostępny przez cały czas, podczas dokonywanych operacji

k) posiadać możliwość definiowania logicznych obiektów zawierających wiele wirtualnych elementów w tym wiele maszyn wirtualnych powiązanych ze sobą zależnościami, tak aby w rezultacie administrator systemu mógł stworzyć wielowarstwowy serwis (np. aplikacja CRM , loadbalance web front-end, middleware oraz sklastrowany back-end baz danych)
l) posiadać możliwość wyboru, które obiekty z katalogu mogą ulegać modyfikacji przez użytkownika końcowego, wymaga się aby lista obiektów była nie mniejsza niż:
    i. liczba wirtualnych procesorów
    ii. wielkość pamięci operacyjnej
    iii. ilość i wielkość dysków oraz typ wolumenu
    iv. ilość kart sieciowych i typy sieci
    v. czas dzierżawy
    vi. polityka archiwizacji
    vii. hasło administracyjne systemu operacyjnego,

    przy czym zmiana parametrów przez użytkownika musi umożliwiać włączenie mechanizmu dodatkowych akceptacji administracyjnych przy procesie uruchomienia serwisu
m) posiadać wsparcie dla dostarczanej platformy wizualizacyjnej
n) posiadać wsparcie dla realizacji modelu: "Projektuj usługę raz, wdrażaj gdziekolwiek"
o) możliwość rezerwacji zasobów fizycznych dla wybranych grup użytkowników oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników
p) mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych, określania dla nich zasobów fizycznych, grup użytkowników, wzorców usług, a także procesów tworzenia oraz zarządzania cyklem życia usług
q) integrować się z innymi systemami zewnętrznymi typu: CMDB, DNS, IPAM, Load Balancer, Servcie Desk, Monitoring, Web Services, Puppet, Chef, SaltStack jako gotowe lub napisane od początku w języku programowania wtyczki (plug-in). Efektem powyższej integracji musi być w pełni automatyczny proces tworzenia i zarządzania usługą niewymagający czynności ręcznych
r) umożliwiać tworzenie nowych usług wraz z określeniem ilości i rodzaju zasobów dostępnych dla danej usługi zarówno na etapie tworzenia jak i późniejszej rekonfiguracji danej usługi
s) posiadać jedno narzędzie do projektowania usługi opartej na systemie operacyjnym, aplikacjach, usługach sieciowych (tj. Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa podczas provisioningu). W sieciowym aspekcie rozwiązanie musi mieć wsparcie dla mikrosegmentacji tj. filtrowania ruchu pomiędzy dowolnymi maszynami wirtualnymi również w obrębie tej samej sieci
t) wspierać natywnie nie mniej niż dwa rozwiązania typu SDN oraz:
    i. umożliwiać zbudowanie zunifikowanego Katalogu Usług dla aplikacji, infrastruktury i danych
    ii. posiadać interfejs typu „drag-drop" przeznaczony do tworzenia dowolnego wielowarstwowego serwisu na podstawie utworzonych wcześniej komponentów,

aplikacji, systemów, sieci i polityk bezpieczeństwa oraz innych skryptów pomocnych w automatyzacji

u) umożliwiać graficzną edycję przebiegu procesu realizacji usług, definiowanie poszczególnych kroków oraz ich danych wejściowych i wyjściowych. Przebiegi procesów mogą być sekwencyjne lub składać się z wielu sekwencji zadań realizowanych równocześnie
v) mieć możliwość testowania zdefiniowanych procesów realizacji usług przy użyciu „debugger-a", który pozwala analizować postęp procesu krok po kroku ze śledzeniem przekazywanych danych
w) umożliwiać eksport/import zdefiniowanych procesów realizacji usług do/z pliku w celu przeniesienia definicji pomiędzy różnymi środowiskami
x) umożliwiać integrację z wykorzystywanym lub planowanym do wykorzystania w projekcie przez Zamawiającego MS Active Directory oraz Open LDAP i wieloma ich domenami w tym samym czasie
y) dawać możliwość użytkownikowi na wykonywania wszystkich operacji na swojej usłudze z jednej konsoli tj. Self-Service portalu bez konieczności posługiwania się innymi narzędziami administracyjnymi
z) posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli – przykładowe role: administrator, architekt usługi, architekt sieci, architekt aplikacji
aa) dostarczać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług za pomocą min. portalu Self-Service i powiadomień e-mail na zdefiniowany adres przez użytkownika/administratora systemu
bb) mieć możliwość zgłaszania przez administratora potrzeby odzyskania poszczególnych zasobów od użytkowników w przypadku ich niewłaściwego wykorzystywania
cc) udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs programistyczny (API).

7.8. Oprogramowanie do monitorowania i zarządzania platformą wirtualizacyjną

1) Zaoferowane oprogramowanie do monitorowania i zarządzania platformą wizualizacyjną musi:
a) uzyskiwać informacje na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością
b) za pomocą wbudowanych inteligentnych algorytmów przewidywać trendy związane z pojemnością środowiska wirtualnego opartego na dostarczanej platformie wirtualizacyjnej
c) posiadać funkcjonalność dającą możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, pamięć RAM, zasoby dyskowe)
d) mieć możliwość tworzenia unikalnego zbioru obiektów korespondujących funkcjami z obiektami centrum danych (ang. Data Center), tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów. Obiekty mogą pochodzić z różnych centrów danych objętych tym rozwiązaniem
e) mieć możliwość tworzenia unikalnego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów z centrów danych w logiczne zbiory dla których będzie istniała

możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów

f) posiadać funkcjonalność tworzenia scenariuszy prognozowanego obliczania pojemności na zasadzie "co jeśli" dla minimum „co jeśli dodamy kolejne maszyn wirtualne”. Rozwiązanie musi umożliwiać definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności musi odnosić się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia
g) posiadać rozwiązanie do generowania alertów na podstawie korelacji (wykrytych podczas monitorowania) anomalii i symptomów, a nie tylko pojedynczych monitorowanych metryk
h) posiadać funkcjonalność dostarczania informacji na temat rekomendowanych, przez wbudowany mechanizm w dostarczanym oprogramowaniu, działań mających na celu prawidłowe działanie dostarczanego środowiska
i) posiadać funkcjonalność obsługi zewnętrznych kolektorów logów i zdarzeń
j) posiadać funkcjonalność monitorowania i zgłaszania alertów na temat zgodności serwerów opartych na dostarczanym rozwiązaniu wirtualizacyjnym mocy obliczeniowej, z najlepszymi praktykami bezpieczeństwa organizacji takich jak ISO (International Organization for Standardization), CIS (Center of Internet Security)
k) posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem zwirtualizowanym
l) wizualizować w trybie online obciążenie środowiska wirtualnego
m) posiadać funkcjonalność graficznej prezentacji monitorowanych parametrów
n) posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich dodatkowego wytwarzania podczas używania oprogramowania
o) dokonywać automatycznej prognozy wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych (wbudowanego w zaoferowane oprogramowanie) oraz planów uruchomienia kolejnych serwerów wirtualnych
p) umożliwiać przeglądanie linii trendu monitorowanych parametrów
q) umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń wirtualnych jak i fizycznych, związanych z dostarczanym oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym
r) umożliwiać monitorowanie środowisk w czasie rzeczywistym (przeglądane informacje powinny ukazywać się w trybie rzeczywistym – dopuszczane jest maksymalne opóźnienie nie większe niż 5 minut)
s) prezentować w formie wykresów/tabel aktualne i historyczne dane dotyczące utylizacji zasobów takich jak CPU, pamięć RAM, zasoby dyskowe oraz interfejsy sieciowe dla każdego systemu operacyjnego
t) umożliwiać przeglądanie wszystkich zbieranych statystyk w postaci wykresów
u) umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, sieć Ethernet, pamięć RAM, zasoby dyskowe)

v) umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków tzw. wąskich gardeł
w) posiadać funkcjonalność zmiany parametrów maszyn wirtualnych, minimum CPU i pamięci RAM, za pomocą wygenerowanego w tym oprogramowaniu zadania. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie w/w zadania – po wygenerowaniu zadanie może być uruchamiane w momencie utworzenia lub w dowolnie skonfigurowanym przez użytkownika czasie
x) posiadać możliwość kasowania, wykonywania kopii migawkowych (ang. snapshot), włączania oraz wyłączania maszyn wirtualnych uruchomionych na monitorowanym środowisku wirtualnym
y) automatycznie przeszukiwać i analizować zebrane dane w celu wynajdywania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, pamięć RAM, zasoby dyskowe) w monitorowanym środowisku
z) posiadać funkcjonalność automatycznego alarmowania o sytuacjach nietypowych – system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o zwiększonym obciążeniu elementu platformy wirtualnej w bieżącym dniu
aa) posiadać możliwość dowolnego przypisywania powiadomień dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie przez użytkownika)
bb) pozwalać na odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z powiązanymi z nimi poradami eksperckimi
cc) umożliwiać definiowanie alertów dla monitorowanego środowiska związanych z:
    i. zarządzaniem pojemnością
    ii. zarządzaniem wydajnością
    iii. anomaliami w środowisku
    iv. zarządzaniu dostępnością
dd) posiadać funkcjonalność przypisania alertu do administratora/operatora rozwiązującego problem
ee) mieć możliwość realizacji funkcji półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra opartego o dostarczone oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej, jak również pomiędzy logicznymi klastrami
ff) integrować się z zaoferowanym oprogramowaniem do centralnego zbierania logów (poprzez integracje zamawiający rozumie możliwość przesyłania danych z oprogramowania do centralnego zbierania logów do zaoferowanego oprogramowania). Zamawiający dodatkowo wymaga, aby konfiguracja dostępu/integracji do/z oprogramowaniem do centralnego zbierania logów odbywała się z konsoli zaoferowanego oprogramowania poprzez podanie danych dostępowych i adresowych do systemu zbierania logów
gg) posiadać funkcjonalność generowania gotowych, predefiniowanych raportów o stanie monitorowanego środowiska
hh) posiadać funkcjonalność pulpitu (ang. dashboard) za pomocą którego administrator będzie posiadał gotowe trzy kolumny z następującymi informacjami:
    i. zdarzenia jakie wystąpiły w zadanym okresie czasu, min. dla: wirtualnych maszyn, sieci wirtualnej
    ii. anomalie jakie wystąpiły w zadanym okresie czasu

iii. zmiany w konfiguracji monitorowanej infrastruktury jakie wystąpiły w zadanym okresie czasu.

Analiza danych ukazująca powyższe wyniki prezentowane na pulpicie musi odbywać się automatycznie poprzez mechanizmy analityczne zaoferowanego oprogramowania do monitorowania na podstawie zakresu czasowego definiowanego przez użytkownika tego pulpitu. Dodatkowo użytkownik musi mieć możliwość definiowania dla którego obiektu, np. wybranej maszyny wirtualnej, należy przeprowadzić analizę, a następnie wyświetlić jej wyniki.

ii) umożliwiać integrację z systemami firm trzecich monitorującymi infrastrukturę
jj) umożliwiać rozbudowę monitorowania dla rozwiązań firm trzecich
kk) umożliwiać konfigurację trybu wysokiej dostępności (ang. HA) dla każdego swojego komponentu w celu uniknięcia awarii pojedynczego elementu
ll) posiadać możliwość zastosowania dodatkowych wtyczek (ang. plugin) odpowiadających za monitorowanie systemów zewnętrznych takich jak m.in: macierze dyskowe, infrastruktury chmurowe, serwery fizyczne, przełączniki LAN umożliwiając tym samym wykorzystanie dedykowanych dodatkowych mechanizmów monitorujących określone komponenty
mm) posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk
nn) posiadać funkcjonalność monitorowania systemów operacyjnych (m.in. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym
oo) posiadać gotowe paczki do monitorowania (ang. management packs) dla komponentów odpowiedzialnych za wirtualizacje sieci, automatyzacje i orkiestrację.
pp) mieć funkcjonalność tworzenia scenariuszy pojemnościowych na zasadzie: "co jeśli" dla minimum: CPU, pamięci RAM oraz przestrzeni dyskowej dla następujących elementów:
    i. dodawania nowych serwerów fizycznych
qq) wykrywać usługi uruchomione na monitorowanych maszynach wirtualnych, a następnie budować relacje lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacji sieciowej
rr) umożliwiać wykonywanie automatycznych działań naprawczych w reakcji na wykryty alarm
ss) posiadać funkcjonalność monitorowania urządzeń firm trzecich typu macierze dyskowe, urządzenia sieciowe, a także innych rozwiązań do wirtualizacji niż dostarczane oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.

7.9. Oprogramowanie do centralnego zbierania logów

Przez logi zamawiający rozumie wszelkie zdarzenia w systemie, które są zapisane do specjalnie przygotowanych plików (dzienników zdarzeń, plików logu) gdzie z każdym pojedynczym wpisem skojarzone są m. in. takie atrybuty jak data wystąpienia zdarzenia, poziom istotności, komunikat zdarzenia.

1) Zaoferowane oprogramowanie do centralnego zbierania logów musi:
a) zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń wykorzystujących rozwiązania typu „syslog"
b) integrować się z oprogramowaniem do monitorowania i zarządzania platformą wirtualizacyjną, opisanym w punkcie **7.8**, w ten sposób, że z poziomu konsoli użytkownika

oprogramowania do monitorowania i zarządzania platformą wirtualizacyjną musi istnieć możliwość uzyskania natychmiastowego dostępu do logów konkretnego urządzenia fizycznego

c) umożliwiać personalizację i wizualizację logów w postaci wykresów co najmniej liniowych, kołowych oraz słupkowych
d) w pełni integrować się z zaoferowanym w tym postępowaniu oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz oprogramowaniem do zarządzania klastrem wirtualizacyjnym
e) zapewnić monitorowanie urządzeń w czasie rzeczywistym
f) posiadać wbudowaną bazę wiedzy dotyczącą logów oraz zdarzeń dla zaoferowanego w tym postępowaniu oprogramowania do wirtualizacji mocy obliczeniowej
g) umożliwiać korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację
h) posiadać możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora
i) umożliwiać przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria
j) posiadać funkcjonalność implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN itp., tak aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej
k) posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów takich jak np.:
    i. logi aplikacji
    ii. logi sieciowe
    iii. pliki konfiguracyjne
    iv. informacje
    v. dane wydajnościowe
    vi. zrzuty awaryjne itp.
    vii. logów „niestrukturalnych”
l) umożliwiać definiowanie struktury dla logów „niestrukturalnych”
m) musi dopuszczać rozłączność uprawnień do interfejsu prezentacji i analizy logów od uprawnień do infrastruktury z której zbierane są logi
n) umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami
o) posiadać możliwość logowania zdarzeń z zaoferowanego oprogramowania dostarczającego zintegrowaną platformę Kubernetes
p) mieć możliwość określania czasu retencji danych, tzn. administrator w konsoli graficznej do zarządzania platformą do zbierania i korelacji logów musi mieć możliwość określenia czasu po jakim zebrane logi będą archiwizowane (eksportowane) na zewnętrzną macierz dyskową. Dodatkowo wymaga się aby retencja mogła być ustawiana granularnie, tj. np. inny czas retencji dla logów z urządzeń klasy firewall, a inny czas retencji dla logów z wirtualizatorów (ang. hypervisor).

7.10. Oprogramowanie dostarczające zintegrowaną platformę Kubernetes

1) Zaoferowane oprogramowanie dostarczające zintegrowaną platformę Kubernetes musi być natywnie uruchamiane na dostarczonym oprogramowaniu do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej.
2) Zamawiający dopuszcza aby zaoferowane oprogramowanie dostarczające zintegrowaną platformę Kubernetes było dostarczone z licencją ograniczoną czasowo. Przy czym licencja ta nie może wygasać wcześniej niż na koniec okresu gwarancji dla Systemu.
3) Zaoferowane oprogramowanie dostarczające zintegrowaną platformę Kubernetes musi:
    a) być certyfikowane przez Cloud Native Computing Foundation (CNCF) w ramach programu certyfikacji zgodności z oprogramowaniem Kubernetes (https://www.cncf.io/certification/software-conformance/)
    b) umożliwiać definiowanie limitów zasobów systemowych takich jak pamięć RAM i moc procesora, które będą dostępne dla całej aplikacji jak i dla poszczególnych kontenerów aplikacji
    c) posiadać LoadBalancer warstwy L4 dostarczany wraz z zamawianym oprogramowaniem, ściśle zintegrowany z platformą oraz wpierany przez producenta oprogramowania
    d) posiadać LoadBalancer realizujący serwisy warstwy L7 takie jak Ingress dostarczany wraz z zamawianym oprogramowaniem, ściśle zintegrowany z platformą oraz wpierany przez producenta oprogramowania
    e) umożliwiać uruchamianie wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych umożliwiając budowanie aplikacji pracujących w oparciu o maszyny wirtualne oraz mikroserwisy
    f) posiadać narzędzia do zarządzania infrastrukturą poprzez interfejs programistyczny platformy Kubernetes – Cluster API
    g) zapewniać środowisko wykonawcze kontenera, które umożliwia interakcję z wtyczkami sieciowymi (w standardzie CNI) i pamięcią masową (w standardzie CSI)
    h) posiadać możliwość wyboru wtyczki sieciowej CNI – co najmniej dwie wtyczki muszą być wspierane, z czego przynajmniej jedna musi umożliwiać integrację z zaoferowanym oprogramowaniem do wirtualizacji sieci, tak aby była możliwość tworzenia polityk bezpieczeństwa z poziomu tego oprogramowania
    i) poprzez zintegrowaną wtyczkę CSI, umożliwiać dostarczanie trwałych zasobów dyskowych, realizowanych bezpośrednio na kompatybilnej z platformą pamięci masowej, co najmniej w trybie pojedynczego odczytu
    j) umożliwiać pracę w środowiskach zamkniętych (ang. air-gapped enviroments)
    k) zawierać wbudowany mechanizm skalowania, który pozwala określić ile instancji danej aplikacji ma być uruchomionych jednocześnie i pozwala na dynamiczne jej modyfikowanie
    l) zawierać wbudowany rejestr obrazów Docker i OCI
    m) umożliwiać integrację z rozwiązaniami CI/CD firm trzecich
    n) umożliwiać przesyłanie logów do zewnętrznych systemów
    o) realizować komunikację pomiędzy aplikacjami i usługami uruchomionymi na platformie poprzez wewnętrzną wirtualną sieć utworzoną w ramach platformy
    p) umożliwiać budowanie i uruchamianie aplikacji stanowych i bezstanowych na bazie orkiestratora Kubernetes

q) oferować integrację z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego systemami takimi jak Microsoft Active Directory/Open LDAP w zakresie dostępu (autoryzacja i uwierzytelnienie) do klastrów Kubernetes
r) umożliwiać izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików
s) umożliwiać konfigurację sieci w taki sposób, żeby poszczególne aplikacje mogły być od siebie sieciowo odizolowane i jakakolwiek komunikacja pomiędzy nimi była zablokowana
t) zapewniać definiowanie uprawnień do poszczególnych obrazów lub grup obrazów dla poszczególnych użytkowników lub grup użytkowników
u) zapewniać możliwość separacji ruchu sieciowego, zasobów sprzętowych, przestrzeni dyskowej pomiędzy różnymi aplikacjami oraz różnymi klastrami Kubernetes
v) umożliwiać definiowanie różnych projektów oraz klastrów Kubernetes dla poszczególnych aplikacji i przypisywania uprawnień do nich dla określonych grup użytkowników
w) mieć możliwość uruchomienia i zarządzania w chmurze prywatnej opartej o dostarczone oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej
x) mieć możliwość zarządzania wersjami i aktualizacjami klastrów Kubernetes, w sposób automatyczny tj. nie powodujący dodatkowych nakładów pracy po stronie administratorów
y) posiadać oprogramowanie do wykonywania kopii zapasowych klastrów Kubernetes – musi istnieć możliwość ograniczania wykonywania kopii danych dla wewnętrznych komponentów klastra Kubernetes tj. wszystkich aplikacji uruchomionych w ramach klastra lub poszczególnych przestrzeni nazw (ang. namespace)
z) zawierać wbudowane mechanizmy automatycznego skalowania aplikacji (uruchamiania lub wyłączania kolejnych instancji aplikacji) w oparciu o metryki zużycia zasobów systemowych przez aplikację
aa) musi zawierać wbudowaną konsolę administracyjną umożliwiającą wykonywanie zadań administracyjnych przez przeglądarkę internetową lub interfejs CLI.
bb) musi zawierać wbudowane narzędzia umożliwiające administrację i konfigurację platformy z poziomu linii poleceń, działające na wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego systemach operacyjnych: Linux, Windows oraz macOS
cc) musi umożliwiać wybór systemu operacyjnego, który jest częścią rozwiązania Kubernetes, wymaga się, aby były wspierane co najmniej dwie dystrybucje systemu typu Linux.

8. Przełączniki sieciowe

Wszystkie zawarte poniżej wymagania są wymaganiami minimalnymi, należy zaoferować urządzenie zapewniające co najmniej podane parametry i funkcje.

l.p	Wymaganie	100GbE	25GbE	1GbE
1	Ilość portów 100GbE (QSFP)	32	8	
2	Ilość portów 1/10GbE (SFP+)			4
3	Ilość portów 1/10/25GbE (SFP28)		48	
4	Ilość portów 10GbE (10GBase-T)			
5	Ilość portów 1GbE (1000Base-T), wykluczając porty dedykowane do zarządzania.			48
6	Interfejsy 100GbE muszą umożliwiać rozdzielenie na cztery interfejsy do pracy z szybkością 25GbE (ang. breakout).	Tak	Tak	Nie
7	Możliwość instalacji modułu optycznego o przepustowości 40 GbE i 25 GbE w interfejsie 100GbE bez zastosowania rozdzielenia interfejsu (ang. breakout).	Tak	Nie	Nie
1	Wysokość przełącznika liczona w jednostkach Rack Units [RU].	1RU	1RU	1RU
2	Przełącznik musi poprawnie pracować w temperaturze od 0 do 40 °C.	Tak	Tak	Tak
3	Przełącznik musi poprawnie pracować przy względnej wilgotności powietrza co najmniej w zakresie od 5% do 90% zakładając brak występowania zjawiska kondensacji pary wodnej.	Tak	Tak	Tak
4	W celu zachowania redundancji zasilania, każdy przełącznik musi poprawnie działać po podłączeniu do dwóch niezależnych, obwodów napięcia przemiennego (AC). Zanik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu przełącznika oraz ograniczenia jego funkcjonalności i	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	1GbE
	wydajności (w zakresie wymaganym przez Zamawiającego). Przełącznik musi być wyposażony w co najmniej dwa zasilacze. Dostarczone zasilacze muszą umożliwiać poprawną pracę przełącznika w pełnej (wymaganej przez Zamawiającego) konfiguracji z wykorzystaniem połowy zainstalowanych zasilaczy.			
5	Przepływ powietrza (związany z działaniem wentylatorów urządzenia) musi odbywać się w kierunku od frontu (porty we/wy) do tyłu urządzenia. **UWAGA**: możliwa zmiana kierunku zgodnie z zapisami w punkcie **10.2.3**, które należy uwzględnić.	Tak	Tak	Tak
6	Przełącznik musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak np. karty z interfejsami sieciowymi, moduły optyczne) w trakcie pracy urządzenia (hot-swap).	Tak	Tak	Tak
7	Przełącznik musi umożliwiać instalację lub wymianę zasilaczy w trakcie pracy urządzenia (hot-swap).	Tak	Tak	Nie
1	Wszystkie przełączniki oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane z wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. end of sale), ani nie może być wiadomym, że urządzenia te nie będą objęte pomocą techniczną producenta (ang. end of life).	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	1GbE
2	Wszystkie przełączniki wraz z działającym na nich oprogramowaniem sterującym muszą pochodzić od jednego producenta.	Tak	Tak	Tak
3	Przełączniki muszą mieć odblokowane wszystkie wymagane funkcjonalności, a jeśli potrzebne są do tego licencje, dostawca musi je dostarczyć wraz z urządzeniami. Licencje nie mogą być ograniczone czasowo, terytorialnie (dotyczy terytorium UE), ani w żaden inny sposób wpływający na cel ich wykorzystania. Restart elementów nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych potrzebnych do odblokowania wszystkich wymaganych funkcjonalności. Licencje powinny być lokalne dla każdego urządzenia – nie dopuszcza się komunikacji z systemami trzecimi w celu utrzymywania/weryfikacji licencji.	Tak	Tak	Tak
4	Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach.	Tak	Tak	Nie
5	Karty, moduły lub porty przełącznika zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi, muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	1GbE
	danego typu interfejsu) pochodzącymi od różnych producentów. Restart przełącznika nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych, które pozwolą na wykorzystywanie modułów optycznych innych producentów. Zastosowanie modułów optycznych innych producentów nie może skutkować utratą, ograniczaniem gwarancji lub wsparcia producenta przełącznika.			
6	Wszystkie przełączniki muszą pracować z tą samą (identyczną) wersją oprogramowania. Oprogramowanie musi być oficjalną wersją oferowaną przez producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby zamawiającego, nieoferowanej innym klientom.	Tak	Tak	Tak
1	Wydajność przełączania co najmniej	6.4 Tbps	4.0 Tbps	290 Gbps
2	Liczba przetwarzanych pakietów na sekundę	2 Bpps	1 Bpps	200 Mpps
3	Czas przełączania ramek nie dłuższy niż	1 µs	1 µs	---
4	Całkowita wielkość buforów	32MB	32MB	4MB
5	Minimalna liczba obsługiwanych adresów MAC	280 000	280 000	30 000
6	Minimalna liczba adresów sieci (nie hostów) IP wersji 4, która musi być zaprogramowana do sprzętowego przełączania pakietów w bazie FIB (ang. Forwarding Information Base).	128 000	128 000	8 000

l.p	Wymaganie	100GbE	25GbE	1GbE
7	Minimalna liczba adresów sieci IP o prefiksie /64 (nie hostów) wersji 6, która musi być zaprogramowana do sprzętowego przełączania pakietów w bazie FIB (ang. Forwarding Information Base).	64 000	64 000	4 000
8	Ilość jednocześnie aktywnych VLANów	4000	4000	1024
9	Całkowita maksymalna moc pobierana przez urządzenie, nie większa niż	650W	650W	250W
10	Typowa moc pobierana przez urządzenie, nie większa niż	400W	400W	250W
1	Moduły optyczne dla interfejsów muszą umożliwiać sprawdzenie mocy odbieranego sygnału.	Tak	Tak	Tak
2	System operacyjny Elementów Przełączających powinien umożliwiać monitorowanie i obrazowanie przetwarzanych pakietów w trybie tekstowym skierowanych do CPU/Modułu zarządzającego – odpowiednik narzędzia Linux TCPDUMP.	Tak	Tak	Nie
3	Przełączniki muszą umożliwiać konfigurację wykorzystując modele OpenConfig. Musi być zapewniona obsługa następujących protokołów: gRPC, RESTCONF, NETCONF.	Tak	Tak	Nie
4	Przełączniki muszą zapewniać strumieniowanie danych telemetrycznych wykorzystując protokół NETCONF/gRPC lub w formacie GPB.	Tak	Tak	Nie
5	Wszystkie przełączniki muszą umożliwiać kopiowanie ruchu z wybranych interfejsów na inny wskazany interfejs (ang. SPAN, Mirroring). Musi istnieć możliwość skonfigurowania minimalnie 4 aktywnych sesji kopiowania ruchu.	Tak	Tak	Nie

l.p	Wymaganie	100GbE	25GbE	1GbE
6	Wszystkie przełączniki muszą obsługiwać protokoły NTP i NTP6.	Tak	Tak	Tak
7	Wszystkie Elementy przełączające muszą wspierać Precision Time Protocol (PTP, IEEE 1588v2).	Tak	Tak	Nie
8	Wszystkie przełączniki muszą obsługiwać protokół LLDP.	Tak	Tak	Tak
9	Wszystkie przełączniki muszą umożliwiać dodanie wydzielonej tablicy routingu dla funkcji zarządzania (ang. Management VRF).	Tak	Tak	Nie
10	Wszystkie przełączniki muszą zapewniać mechanizm sprzętowej ochrony przeciw atakowi przeciążającemu (ang. DoS) na jednostkę sterującą CPU (ang. Control Plane Protection).	Tak	Tak	Nie
1	Przełączniki muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie przy enkapsulacji musi być możliwa obsługa przełączania w warstwie L2 (ang. bridging).	Tak	Tak	Nie
2	Przełączniki muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie, przy enkapsulacji musi być możliwa obsługa routingu IP.	Tak	Tak	Nie
3	Przełączniki muszą obsługiwać MP- BGP EVPN (Ethernet VPN) jako mechanizm sygnalizacyjny (ang. control-plane) dla enkapsulacji VXLAN. Musi być zapewniona obsługa L2 EVPN (Type-2), L3-EVPN (type-5) oraz jednoczesna obsługa routingu i bridging'u IRB.	Tak	Tak	Nie
4	Przełączniki muszą obsługiwać mechanizm protekcji grup linków Ethernet (LAG z LACP) poprzez podłączenie ich do co najmniej dwóch Elementów przełączających. To znaczy, pojedyncza wiązka LAG musi mieć	Tak	Tak	Nie

l.p	Wymaganie	100GbE	25GbE	1GbE
	możliwość zakończenia na co najmniej dwóch Elementach przełączających zapewniając w pełni aktywną komunikację na wszystkich linkach grupy. Protekcja musi zapewniać nieprzerwaną pracę w przypadku awarii dowolnego pojedynczego komponentu. Protekcja musi poprawnie współpracować z VXLAN, EVPN, SpanningTree. Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m			
1	Wszystkie przełączniki muszą obsługiwać ramki Ethernet o wielkości co najmniej 9216 Bytes. Liczonej łącznie z preambułą (7 oktetów), polem FCS (4 oktety), Frame Delimiter (1 oktet) i Interframe Gap (12 oktetów).	Tak	Tak	Tak
2	Wszystkie przełączniki muszą obsługiwać funkcję IGMP snooping (dla IGMPv2 oraz IGMPv3).	Tak	Tak	Tak
3	Wszystkie przełączniki muszą obsługiwać agregację interfejsów z wykorzystaniem protokołu LACP (IEEE 802.3ad).	Tak	Tak	Tak
4	Wszystkie przełączniki muszą umożliwiać stworzenie protekcji terminującej zagregowane interfejsy (LAG) na dwu Elementach przełączających (ang. Dual Homing). W ramach takiej protekcji wszystkie porty zagregowanego połączenia LAG muszą aktywnie przenosić dane (ang. Active/Active). Awaria jednego Elementu nie może wpływać na status	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	1GbE
	połączenia zagregowanego. Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m.			
5	Wszystkie przełączniki muszą obsługiwać 802.1w RSTP, 802.1s MSTP.	Tak	Tak	Tak
6	Wszystkie przełączniki muszą umożliwiać tworzenie list bezpieczeństwa (ang. ACLs) na warstwie L2 (MAC ACL), warstwie L3 (IP) i warstwie L4 (porty).	Tak	Tak	Tak
7	Wszystkie przełączniki muszą obsługiwać protokół 802.1Qbb PFC (Priority-based Flow Control).	Tak	Tak	Nie
8	Wszystkie przełączniki muszą umożliwiać regulację (ang. Shaping) wielkości ruchu wyjściowego.	Tak	Tak	Nie
9	Wszystkie przełączniki zapewniać statyczny routing IP oraz dynamiczny routing IP zgodny z OSFPv2, OSFPv3, BGP.	Tak	Tak	Tak
10	Wszystkie przełączniki muszą zapewniać mechanizm dystrybucji pakietów IP poprzez ścieżki z równym kosztem (ang. Equal Cost Multi-Path routing ECMP).	Tak	Tak	Tak
11	Wszystkie przełączniki muszą zapewniać możliwość tworzenia polityk dla routing IP (ang. Route Maps).	Tak	Tak	Nie
12	Wszystkie przełączniki muszą zapewniać możliwość dystrybucji informacji routingowych pomiędzy różnymi wirtualnymi tablicami routingowymi (ang. VRF route leaking).	Tak	Tak	Nie
13	Wszystkie przełączniki muszą obsługiwać protokół BFD.	Tak	Tak	Nie

9. Stacje graficzne

9.1. Stacja Graficzna Typ 1

Pojedyncza Stacja Graficzna Typ 1 składa się z następujących części składowych:

9.1.1. Jednostka główna spełniająca poniższe wymagania:

1) Wyświetlacz: 14” cala, rozdzielczość 1920x1200, jasność min. 500 nit, 100% sRGB z powłoką przeciwodblaskową i technologią niskiej emisji niebieskiego światła (ang. Low Blue Light);
2) Procesor: zgodny z x64, posiadający co najmniej 14 fizycznych rdzeni, co najmniej 20 wątków. Zaprojektowany do pracy w mobilnych stacjach roboczych (pobór mocy w podstawowym trybie pracy nie więcej niż 45W), co najmniej 24MB cache, osiągający wydajność minimum: 30500 punktów Passmark CPU Mark w teście wydajności Pass Mark Perfomance Test (stan na 22.06.2023) pracujący z minimalną częstotliwością w trybie turbo 5,4GHz;
3) Pamięć RAM: nie mniej niż 64 GB;
4) Karta graficzna z pamięcią min. 4 GB,
5) Dysk twardy M.2 SSD NVMe: min. 1TB;
6) Zintegrowane porty (co najmniej):
   a) min. 4x gniazdo Thunderbolt 4 (USB Type-C) z obsługą PowerDelivery i DisplayPort,
   b) zintegrowany czytnik kart microSD,
   c) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm,
7) Komunikacja:
   a) Wi-Fi min. 6E,
   b) Bluetooth.
8) Bateria: nie mniej niż 70Wh, przy czym Zamawiający dopuszcza odchylenia od podanej wartości o +/- 5%.;
9) Waga: nie więcej niż 1,55 kg.;
10) Dodatkowe wymagania:
    a) klawiatura: QWERTY, podświetlana,
    b) Touchpad,
    c) co najmniej dwa wbudowane głośniki oraz mikrofon,
    d) wbudowana kamera o rozdzielczości min. 720p z funkcją IR,
    e) zintegrowany czytnik linii papilarnych,
    f) dedykowany przez producenta zasilacz z wtyczką USB Type-C z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL,
    g) wbudowany moduł TPM (Trusted Platform Module),
    h) zestaw funkcji wbudowanych w płytę główną komputera i innych podzespołów zapewniających kombinację technologii zawartych w procesorze, usprawnień sprzętowych, funkcji zarządzających i zabezpieczających. Zapewnia on zdalny dostęp do komputera wliczając monitoring, sterowanie nim, konserwację niezależnie od stanu systemu operacyjnego nawet wtedy, gdy komputer jest wyłączony, w szczególności w zakresie:

i. inwentaryzacji zasobów systemowych,
ii. zdalnego włączenie/wyłączenie/restart komputera poprzez TCP/IP,
iii. zdalnego diagnozowania - zdalna konsola tekstowa do BIOSu i konsola graficznej (KVM),
iv. obsługi moduł TMP,
v. zdalna konfiguracja BIOS, zdalny update BIOS,
vi. zdalne monitorowanie stanu komponentów komputera – m.in. CPU, pamięć, dysk itp.,
vii. możliwość zdalnej blokady komputera w przypadku kradzieży sprzętowego. Jedynym warunkiem jest podłączenie komputera do sieci komputerowej oraz do zasilania.

11) System operacyjny: Licencja na system Windows 11 Professional PL 64-bit lub równoważny.
12) Wsparcie producenta dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego następujących systemów operacyjnych:
    a) Microsoft Windows 11 Pro 64-bit,
    b) Ubuntu Linux,
13) Bezpłatne oprogramowanie do automatycznej diagnostyki z funkcją przewidywania usterek dysków twardych oraz baterii laptopa, i informowania o nich zanim wystąpią awarie. Musi posiadać co najmniej poniższą funkcjonalność:
    a) monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów,
    b) powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu,
    c) powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów.

9.1.2. Monitor

Kompatybilny ze Stacją Graficzną Typu 1 monitor LCD 27” 4K ze złączem USB Type-C o następującej parametrach technicznych:

a) przekątna „27” w formacie 16:9,
b) rozdzielczość min. 3840 x 2160,
c) matowa matryca IPS,
d) kontrast min. 2000:1,
e) jasność min. 400 cd/m^2
f) czas reakcji monitora – nie więcej niż 5 ms,
g) paleta kolorów – 100% Rec 709, 100% sRGB, min. 98% DCI-P3
h) kąty widzenia: min. 178° w pionie i poziomie,
i) złącza (gniazda) co najmniej: min. 1x HDMI , min. 1x DisplayPort min. 1.4, 1x wyjście DisplayPort (dla monitora z obsługą MST (Multi-Stream Transport), min. 1x USB Type-C do podłączenia z komputerem (z funkcją ładowania laptopa z mocą min. 90W oraz DisplayPort), RJ45 (Ethernet), min 4x USB w standardzie min. 3.2 Gen 2;
j) funkcje: funkcja obrotowego ekranu (PIVOT -90° /+90°), regulacja wysokości (min. 150mm), regulacja kąta pochylenia (w zakresie min. -5° /+20°)

k) dołączone przewody (min): 1 x kabel z wtyczkami DisplayPort-DisplayPort, 1 x kabel z wtyczkami USB Type-C – USB Type-C, 1 x kabel z wtyczkami USB Type-C – USB Type-A,
l) zasilanie – napięcie 100-240VAC,
m) z monitorem musi zostać dostarczony przewód umożliwiającym zasilanie z gniazdek używanych na terenie PL,

9.1.3. Stacja dokująca

Stacja dokująca kompatybilna ze Stacją Graficzną Typu 1 podłączana poprzez Thunderbolt 4 (USB Type-C) za pomocą złącza USB Type-C. Musi być wyposażona co najmniej w następujące złącza (gniazda):

a) 1x USB Type-C w standardzie co najmniej USB 3.2 Gen 2,
b) 3x USB Type-A w standardzie co najmniej 3.2 Gen 1 w tym co najmniej 1 z funkcjonalnością PowerShare
c) 2x DisplayPort 1.4,
d) 1x HDMI min. 2.0,
e) 1x USB-C w standardzie co najmniej USB 3.2 Gen 2 z funkcją DisplayPort 1.4
f) 1x LAN 10/100/1000 Ethernet (RJ-45)
g) 2x Thunderbolt 4 w postaci złącza USB Type-C,
h) gniazdo do podłączenia zewnętrznego dedykowanego do stacji dokującej zasilacza

Stacja dokująca musi być wyposażona w 1 wtyczkę Thunderbolt 4 w postaci złącza USB Type-C, do podłączenia komputera, na kablu o długości min. 0,5m.

Stacja musi zapewnić poprawną pracę z 3 monitorami w rozdzielczość 4K.
Ze stacją musi zostać dostarczony dedykowany do niej zasilacz, zapewniający zasilanie podłączonego do stacji dokującej komputera mocą min. 90W (130W w przypadku podłączenie komputera, którego producentem jest producent stacji dokującej) z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL. Wymagane jest aby dostarczane poprzez stację dokującą zasilanie było wystarczające do poprawnej pracy Stacji Graficznej Typu 1 bez potrzeby podłączania jej do dodatkowego zasilania.
Dodatkowa wymagana poprawna obsługa: PXE Boot, Wake-On-LAN, Wake-On-Dock.
Stacja dokująca musi poprawnie współpracować z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego następującymi systemami operacyjnymi: Windows 11, Ubuntu Linux.

9.1.4. Zestaw klawiatura z myszą

1) Kompatybilny ze Stacją Graficzną Typu 1 zestaw klawiatury i myszy.
2) Musi posiadać następującą funkcjonalność:
    a) zasilanie za pomocą baterii lub akumulatorów - poprawność pracy na jednym komplecie baterii 36 miesięcy,
    b) możliwość jednoczesnego bezprzewodowego podłączenia do trzech różnych komputerów – jednego za pomocą odbiornika USB, pozostałych dwóch za pomocą Bluetooth. Przełączania pomiędzy poszczególnymi komputerami muszą być realizowane przy użyciu klawisza lub przycisku na klawiaturze lub myszy.

Aktualne podłączone urządzenie musi być sygnalizowane za pomocą dedykowanej diody zarówno na klawiaturze jak i na myszy,

c) układ klawiatury QWERTY US międzynarodowy z oddzielnym blokiem numerycznym oraz klawiszami strzałek i klawiszami funkcyjnymi,
d) mysz z optyczną technologią wykrywania ruchu obsługującą rozdzielczość min. 1000dpi,
e) poprawna współpraca z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego systemami: Microsoft Windows 11, Ubuntu Linux.

3) Do zestawu muszą zostać dołączone baterie w liczbie i modelu umożliwiającym poprawną pracę zestawu.

9.2. Stacja Graficzna Typ 2

Pojedyncza Stacja Graficzna Typ 1 składa się z następujących części składowych:

9.2.1. Jednostka główna spełniająca poniższe wymagania:

1) Wyświetlacz: 16” cala, rozdzielczość 3840 x 2400, jasność min. 400 nit, 100% DCIP3, OLED;
2) Procesor: zgodny z x64, posiadający co najmniej 24 fizycznych rdzeni, co najmniej 32 wątków. Zaprojektowany do pracy w mobilnych stacjach roboczych (pobór mocy w podstawowym trybie pracy nie więcej niż 55W), co najmniej 32MB cache, osiągający wydajność minimum: 45000 punktów Passmark CPU Mark w teście wydajności Pass Mark Perfomance Test (stan na 22.06.2023) pracujący z minimalną częstotliwością w trybie turbo 5,5GHz;
3) Pamięć RAM: nie mniej niż 128 GB;
4) Karta graficzna z pamięcią min. 16 GB,
5) Dysk twardy – zainstalowane 3 dyski M.2 SSD NVMe:
   a. dysk nr 1 o pojemności min. 2TB;
   b. dysk nr 2 o pojemności min. 4TB;
   c. dysk nr 3 o pojemności min. 512GB;
6) Zintegrowane porty (co najmniej):
   a) 2x gniazdo Thunderbolt 4 (USB Type-C) z obsługą PowerDelivery i DisplayPort,
   b) USB-C w standardzie co najmniej USB 3.2
   c) 2x USB Type-A w standardzie co najmniej USB 3.2
   d) HDMI
   e) zintegrowany czytnik kart SD,
   f) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm,
7) Komunikacja:
   a) 1x LAN 10/100/1000 Ethernet (RJ-45)
   b) Wi-Fi min.6E,
   c) Bluetooth.
8) Bateria: nie mniej niż 90Wh, przy czym Zamawiający dopuszcza odchylenia od podanej wartości o +/- 5%.;

9) Waga: nie więcej niż 3 kg
10) Dodatkowe wymagania:
    a) klawiatura: QWERTY, podświetlana,
    b) Touchpad,
    c) co najmniej dwa wbudowane głośniki oraz mikrofon,
    d) wbudowana kamera HD o rozdzielczości min. 1080p z funkcją IR,
    e) zintegrowany czytnik linii papilarnych,
    f) wbudowane gniazdo czytnika kart SmartCard Reader,
    g) wbudowany czytnik kart SmartCard Reader/NFC,
    h) dedykowany przez producenta zasilacz z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL,
    i) wbudowany moduł TPM (Trusted Platform Module),
    j) zestaw funkcji wbudowanych w płytę główną komputera i innych podzespołów zapewniających kombinację technologii zawartych w procesorze, usprawnień sprzętowych, funkcji zarządzających i zabezpieczających. Zapewnia on zdalny dostęp do komputera wliczając monitoring, sterowanie nim, konserwację niezależnie od stanu systemu operacyjnego nawet wtedy, gdy komputer jest wyłączony, w szczególności w zakresie:
        viii. inwentaryzacji zasobów systemowych,
        ix. zdalnego włączenie/wyłączenie/restart komputera poprzez TCP/IP,
        x. zdalnego diagnozowania - zdalna konsola tekstowa do BIOSu i konsola graficznej (KVM),
        xi. obsługi moduł TMP,
        xii. zdalna konfiguracja BIOS, zdalny update BIOS,
        xiii. zdalne monitorowanie stanu komponentów komputera – m.in. CPU, pamięć, dysk itp.,
        xiv. możliwość zdalnej blokady komputera w przypadku kradzieży sprzętowego. Jedynym warunkiem jest podłączenie komputera do sieci komputerowej oraz do zasilania.
11) System operacyjny: Licencja na system Windows 11 Professional PL 64-bit lub równoważny.
12) Wsparcie producenta dla wykorzystywanych lub planowanych do wykorzystania w projekcie przez Zamawiającego następujących systemów operacyjnych:
    a) Microsoft Windows 11 Pro 64-bit,
    b) Ubuntu Linux,
13) Bezpłatne oprogramowanie do automatycznej diagnostyki z funkcją przewidywania usterek dysków twardych oraz baterii laptopa, i informowania o nich zanim wystąpią awarie. Musi posiadać co najmniej poniższą funkcjonalność:
    a) monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów,
    b) powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu,
    d) powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów..

9.2.2. Monitor

Kompatybilny ze Stacją Graficzną Typu 2 monitor LCD 27” 4K ze złączem USB Type-C o następującej parametrach technicznych:

a) matryca min. 26,90" w formacie 16:9,
b) rozdzielczość 3840 x 2160,
c) matowa matryca IPS,
d) kontrast min. 1400:1,
e) jasność min. 500 cd/m^2
f) czas reakcji monitora – nie więcej niż 13 ms,
g) obsługa kolorów – min. 1 miliard (wyświetlanie 10-bitowe) z palety 278 bilionów (16-bitowa tabela LUT);
h) paleta kolorów – min. 99% Adobe RGB, min. 98% DCI-P3
i) kąty widzenia: min. 178° w pionie i poziomie,
j) złącza (gniazda) co najmniej:
   min. 1x HDMI,
   min. 1x DisplayPort,
   min. 1x USB Type-C do podłączenia z komputerem (z funkcją ładowania laptopa z mocą 94 W oraz DisplayPort),
   min 2x USB w standardzie min. 3.1,
   1x Ethernet (RJ-45 1000BASE-T)
k) funkcje: stabilizacja jasności, predefiniowane tryby pracy (min. AdobeRGB, sRGB), regulacja koloru, krzywa PQ (Perceptual Quantization), krzywa HLG (Hybrid Log-Gamma), autokalibracja za pomocą wbudowanego kalibratora, format koloru wejściowego, model kolorów YUV, zakres sygnału wejściowego, konwersja I/P, powiększanie obrazu (za pomocą przycisków na monitorze), tryb DCI 4K Cropping, tryb BT.709 Gamut Warning, tryb Luminance Warning, pomijanie sygnału wejściowego, pomijanie trybu wyświetlania, funkcja DUE Priority
l) funkcje fizyczne: funkcja obrotowego ekranu (PIVOT 90°), regulacja wysokości (min. 150mm), regulacja kąta pochylenia (w zakresie min. dół 5° /góra 35°), możliwość obrotu w zakresie min. 340°
m) dołączone akcesoria: dedykowany przez producenta monitora kaptur zapobiegający odbijaniu się światła od powierzchni ekranu montowany magnetycznie do monitora; przewody (min): 1 x kabel z wtyczkami USB Type-C – USB Type-C, 1 x kabel z wtyczkami USB Type-A – USB Type-B, 1 x kabel z wtyczkami HDMI – HDMI
n) zasilanie – napięcie 100-240VAC,
o) z monitorem musi zostać dostarczony przewód umożliwiającym zasilanie z gniazdek używanych na terenie PL,

9.2.3. Stacja dokująca

Stacja dokująca kompatybilna ze Stacją Graficzną Typu 2 podłączana poprzez podwójny kable USB Type-C za pomocą złącza USB Type-C. Musi być wyposażona co najmniej w następujące złącza (gniazda):

a) 3x USB Type-A w standardzie co najmniej USB 3.1,
b) 2x DisplayPort 1.4,
c) 1x HDMI,
d) 2x USB-C w standardzie co najmniej USB 3.1 Gen 2, w tym co najmniej jedno z funkcją DisplayPort 1.4
e) 1x LAN 10/100/1000 Ethernet (RJ-45)
f) gniazdo do podłączenia zewnętrznego dedykowanego do stacji zasilacza

Stacja dokująca musi być wyposażona w 2 wtyczki USB-C w postaci złącz USB Type-C, do podłączenia komputera, na kablu o długości min. 0,5m.

Stacja musi zapewnić poprawną pracę z 2 monitorami w rozdzielczość 4K.
Ze stacją musi zostać dostarczony dedykowany do niej zasilacz, zapewniający zasilanie podłączonego do stacji dokującej komputera o mocy min. 90W (210W w przypadku podłączenie komputera, którego producentem jest producent stacji dokującej przy wykorzystaniu dwóch złącz USB-C) z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL. Wymagane jest aby dostarczane poprzez stację dokującą zasilanie było wystarczające do poprawnej pracy Stacji Graficznej Typu 2 bez potrzeby podłączania jej do dodatkowego zasilania.
Dodatkowa wymagana poprawna obsługa: PXE Boot, Wake-On-LAN, Wake-On-Dock.

9.2.4. Zestaw klawiatura z myszą

1) Kompatybilny ze Stacją Graficzną Typu 2 zestaw klawiatury i myszy.
2) Musi posiadać następującą funkcjonalność:
   a) zasilanie za pomocą baterii lub akumulatorów - poprawność pracy na jednym komplecie baterii 36 miesięcy,
   b) możliwość jednoczesnego bezprzewodowego podłączenia do trzech różnych komputerów – jednego za pomocą odbiornika USB, pozostałych dwóch za pomocą Bluetooth. Przełączania pomiędzy poszczególnymi komputerami muszą być realizowane przy użyciu klawisza lub przycisku na klawiaturze lub myszy. Aktualne podłączone urządzenie musi być sygnalizowane za pomocą dedykowanej diody zarówno na klawiaturze jak i na myszy,
   c) układ klawiatury QWERTY US międzynarodowy z oddzielnym blokiem numerycznym oraz klawiszami strzałek i klawiszami funkcyjnymi,
   d) mysz z optyczną technologią wykrywania ruchu obsługującą rozdzielczość min. 1000dpi,
   e) poprawna współpraca z wykorzystywanymi lub planowanymi do wykorzystania w projekcie przez Zamawiającego systemami: Microsoft Windows 11, Ubuntu Linux.
3) Do zestawu muszą zostać dołączone baterie w liczbie i modelu umożliwiającym poprawną pracę zestawu.

9.3. Opis równoważności

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez Wykonawcę jako równoważne dla systemu operacyjnego Windows 11 Professional PL 64-bit lub równoważny.

Przez równoważność Zamawiający rozumie konieczność:

1. zapewnienia przez system pełnej funkcjonalności jaką oferuje system Windows w minimalnej wskazanej przez Zamawiającego wersji,
2. dostępność dla systemu równoważnego tych aplikacji oraz oprogramowania, które są dostępne dla wskazanego przez Zamawiającego systemu Windows lub aplikacji i oprogramowań alternatywnych, zapewniających wszystkie te same funkcjonalności.

10. Wdrożenie systemu

W ramach wdrożenia Systemu Wykonawca zobowiązany jest do:

1) realizacji planu wdrożenia zawartego w punkcie **10.1**
2) dostawy przedmiotu zamówienia zgodnie z Załącznikiem nr 1 do SWZ
3) dostawy, instalacji i konfiguracji urządzeń w siedzibie Zamawiającego:
   PCSS – Poznańskie Centrum Superkomputerowo-Sieciowe, Budynek Sal Technologicznych (BST) ul. Jana Pawła II 10, 61-139 Poznań

10.1. Ramowy plan wdrożenia

Plan realizacji przedmiotu zamówienia:

Lp.	Element wdrożenia	Dni robocze* (terminy maksymalne)
OPRACOWANIE DOKUMENTACJI TECHNICZNEJ		
1.	Wykonanie Dokumentacji Technicznej zgodnie z wytycznymi zawartymi w punkcie **10.4**	10 dni od daty złożenia zapotrzebowania przez zamawiającego, ale przed rozpoczęciem dostawy (Zgodnie z załączonym wykresem Gantta)
2.	Weryfikacja dokumentacji technicznej przez Zamawiającego	10 dni roboczych od dnia jej dostarczenia przez wykonawcę (Zgodnie z załączonym wykresem Gantta)
3.	Naniesienie poprawek w dokumentacji technicznej przez Wykonawcę zgodnie z wytycznymi Zamawiającego	5 dni roboczych od dnia zgłoszenia konieczności dokonania poprawek przez zamawiającego (Zgodnie z załączonym wykresem Gantta)
DOSTAWA I INSTALACJA SYSTEMU		

4.	Dostawa urządzeń i oprogramowania	30 dni roboczych od daty złożenia zapotrzebowania przez zamawiającego. (Zgodnie z załączonym wykresem Gantta)
5.	Instalacja i konfiguracja obejmująca 4 etapy: 1. Instalacja urządzeń w szafach telekomunikacyjnych zlokalizowanych w obiektach Zamawiającego wraz z ułożeniem okablowania i podłączenie urządzeń do przełączników sieciowych i zasilania. 2. Instalacja i konfiguracja logiczna całego środowiska (serwery wraz z systemem do zarządzania, macierze, systemy pamięci masowej, urządzenie do przechowywania kopii zapasowych, platforma wirtualizacyjna wraz z modułami, przełączniki sieciowe, pozostałe elementy) zgodnie z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną. 3. Konfiguracja Systemu obejmująca konfigurację i uruchomienie platformy wirtualizacyjnej oraz oprogramowania do wykonywania kopii zapasowych w sposób zgodny z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną. 4. Przygotowanie i przeprowadzenie przez Wykonawcę testów weryfikacyjnych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie **10.6.1** z Części IV SWZ. Przygotowanie raportu podsumowującego wyniki testów.	10 dni roboczych od daty dostarczenia urządzeń i oprogramowania do zamawiającego (Zgodnie z załączonym wykresem Gantta)
OPRACOWANIE DOKUMENTACJI POWYKONAWCZEJ		
6.	Wykonanie Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi w punkcie **10.5**	1 dzień roboczy, najpóźniej w dniu zakończeniu instalacji i konfiguracji Systemu u zamawiającego (Zgodnie z załączonym wykresem Gantta)
7.	Weryfikacja Dokumentacji Powykonawczej przez Zamawiającego	1 dzień roboczy od dnia jej dostarczenia przez wykonawcę

		(Zgodnie z załączonym wykresem Gantta)
8.	Naniesienie poprawek do Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi Zamawiającego	1 dzień roboczy od dnia zgłoszenia konieczności dokonania poprawek przez zamawiającego (Zgodnie z załączonym wykresem Gantta)
WERYFIKACJA POPRAWNOŚCI INSTALACJI SYSTEMU (PRZEPROWADZENIE TESTÓW)		
9.	Przygotowanie przez Wykonawcę planu testów akceptacyjnych i wydajnościowych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie **10.6.2** i **10.6.3**	3 dni robocze, najpóźniej 1 dzień przed zakończeniem instalacji i konfiguracji Systemu u zamawiającego (Zgodnie z załączonym wykresem Gantta)
10.	Weryfikacja planu testów akceptacyjnych i wydajnościowych przez Zamawiającego	1 dzień roboczy od dnia jego dostarczenia przez wykonawcę, najpóźniej w dniu zakończenia instalacji i konfiguracji Systemu u zamawiającego (Zgodnie z załączonym wykresem Gantta)
11.	Naniesienie poprawek na planie testów akceptacyjnych i wydajnościowych przez Wykonawcę zgodnie z wytycznymi Zamawiającego	1 dzień roboczy od dnia zgłoszenia konieczności dokonania poprawek przez zamawiającego (Zgodnie z załączonym wykresem Gantta)
12.	Wykonanie przez Wykonawcę testów akceptacyjnych i wydajnościowych oraz wykonanie raportu podsumowującego wyniki testów wraz ze zgłoszeniem gotowości do testów odbiorczych	2 dni robocze (Zgodnie z załączonym wykresem Gantta)
13.		1 dzień roboczy od zgłoszenia gotowości

	Przygotowanie przez Wykonawcę planu testów odbiorczych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie **10.6.4**	do testów odbiorczych u zamawiającego (Zgodnie z załączonym wykresem Gantta)
14.	Weryfikacja planu testów odbiorczych przez Zamawiającego	1 dzień roboczy od dnia jego dostarczenia przez wykonawcę (Zgodnie z załączonym wykresem Gantta)
15.	Naniesienie poprawek na planie testów odbiorczych przez Wykonawcę zgodnie z wytycznymi Zamawiającego	1 dzień roboczy od dnia zgłoszenia konieczności dokonania poprawek przez zamawiającego (Zgodnie z załączonym wykresem Gantta)
16.	Wykonanie testów odbiorczych przez Wykonawcę i Zamawiającego i wykonanie przez Wykonawcę raportu podsumowującego wyniki testów	2 dni robocze (Zgodnie z załączonym wykresem Gantta)
17.	Podpisanie przez Zamawiającego protokołu zdawczo - odbiorczego przedmiotu zamówienia	1 dzień roboczy po pozytywnym zakończeniu testów odbiorczych u zamawiającego (Zgodnie z załączonym wykresem Gantta)

*przez „dzień roboczy" Zamawiający rozumie poniedziałek, wtorek, środę, czwartek i piątek z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Poniżej przedstawiono ramowy plan wdrożenia w skali czasu (wykres Gantta)

Lp	Czynności	Dni robocze
I	**Podpisanie umowy**	
II	**Złożenie zapotrzebowania**	
III	**Opracowanie Dokumentacji Technicznej**	
1	Wykonanie Dokumentacji Technicznej zgodnie z wytycznymi zawartymi w punkcie 10.4	
2	Weryfikacja dokumentacji technicznej przez Zamawiającego	
3	Naniesienie poprawek w dokumentacji technicznej przez Wykonawcę zgodnie z wytycznymi Zamawiającego	
IV	**Dostawa i instalacja systemu**	
4	Dostawa urządzeń i oprogramowania	
5	Instalacja i konfiguracja obejmująca 3 etapy: 1. Instalacja urządzeń w szafach telekomunikacyjnych zlokalizowanych w obiektach Zamawiającego wraz z ułożeniem okablowania i podłączenie urządzeń do przełączników sieciowych i zasilania. 2. Instalacja i konfiguracja logiczna całego środowiska (serwery wraz z systemem do zarządzania, macierze, systemy pamięci masowej, urządzenie do przechowywania kopii zapasowych, platforma wirtualizacyjna wraz z modułami, przełączniki sieciowe, pozostałe elementy) zgodnie z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną. 3. Konfiguracja Systemu obejmująca konfigurację i uruchomienie platformy wirtualizacyjnej oraz oprogramowania do wykonywania kopii zapasowych w sposób zgodny z wykonaną wcześniej przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną. 4. Przygotowanie i przeprowadzenie przez Wykonawcę testów weryfikacyjnych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 10.6.1 z Części IV SWZ. Przygotowanie raportu podsumowującego wyniki testów	
V	**Opracowanie Dokumentacji Powykonawczej**	
6	Wykonanie Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi w punkcie 10.5	
7	Weryfikacja Dokumentacji Powykonawczej przez Zamawiającego	
8	Naniesienie poprawek do Dokumentacji Powykonawczej przez Wykonawcę zgodnie z wytycznymi Zamawiającego	
VI	**Weryfikacja Poprawności instalacji systemu (przeprowadzenie testów)**	
9	Przygotowanie przez Wykonawcę planu testów akceptacyjnych i wydajnościowych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 10.6.2 i 10.6.3	
10	Weryfikacja planu testów akceptacyjnych i wydajnościowych przez Zamawiającego	
11	Naniesienie poprawek na planie testów akceptacyjnych i wydajnościowych przez Wykonawcę zgodnie z wytycznymi Zamawiającego	
12	Wykonanie przez Wykonawcę testów akceptacyjnych i wydajnościowych oraz wykonanie raportu podsumowującego wyniki testów wraz ze zgłoszeniem gotowości do testów odbiorczych	
13	Przygotowanie przez Wykonawcę planu testów odbiorczych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 10.6.4	
14	Weryfikacja planu testów odbiorczych przez Zamawiającego	
15	Naniesienie poprawek na planie testów odbiorczych przez Wykonawcę zgodnie z wytycznymi Zamawiającego	
16	Wykonanie testów odbiorczych przez Wykonawcę i Zamawiającego i wykonanie przez Wykonawcę raportu podsumowującego wyniki testów	
17	Podpisanie przez Zamawiającego protokołu zdawczo - odbiorczego przedmiotu zamówienia	

10.2. Dostawa i instalacja

Wykonawca zobowiązany jest dostarczyć wszelkie urządzenia i oprogramowanie będące przedmiotem zamówienia do lokalizacji Zamawiającego oraz wykonania ich fizycznej instalacji w tej lokalizacji z uwzględnieniem warunków opisanych poniższych podpunktach (**10.2.1**, **10.2.2**, **10.2.3**).

10.2.1. Ogólne wytyczne dotyczące dostawy i instalacji

1) Termin każdej dostawy musi zostać uzgodniony z Zamawiającym.
2) Wykonawca zobowiązany jest do zgłoszenia terminu dostawy na co najmniej 5 dni przed planowanym terminem dostawy.
3) Wykonawca zobowiązany jest do wskazania osoby nadzorującej realizację przedmiotu zamówienia.
4) Wykonawca zobowiązany jest do dostarczenia i montażu urządzeń do lokalizacji Zamawiającego. Dostawę Wykonawca musi zrealizować własnym sprzętem oraz zobowiązany jest do pokrycia wszelkich kosztów związanych z transportem, montażem i ubezpieczeniem dostawy.
5) Prace objęte umową prowadzone będą w obiektach udostępnionych Wykonawcy i pod nadzorem Zamawiającego.
6) Wykonawca zobowiązany jest do prowadzenia na bieżąco prac porządkowych, zarówno w pomieszczeniach objętych montażem jak i na trasie transportu materiałów oraz sprzątanie po wykonaniu każdego etapu prac. Wywóz odpadów należy zrealizować we własnym zakresie (kartony, palety, odpady materiałowe itp.), przy czym odpady można składować w kontenerze nie większym niż 1,7 m3 chyba, że na etapie realizacji zostanie to ustalone inaczej.
7) Wykonawca zobowiązany jest do przestrzegania przepisów porządkowych obowiązujących na terenie budynku Zamawiającego.
8) Zamawiający wymaga, aby pracownicy Wykonawcy oraz jego podwykonawcy przebywali na terenie prowadzenia prac w ubraniach roboczych jednoznacznie identyfikujących firmę dla jakiej pracują (mogą to być np. koszulki odblaskowe z nazwą Wykonawcy). Za każdorazowe nieprzestrzeganie tego wymogu zostanie naliczona kara w wysokości 500,00 zł.
9) Zabronione jest palenie tytoniu oraz używanie innych substancji wonnych (np. papierosy elektroniczne) na terenie wszystkich obiektów Zamawiającego, w których realizowany jest przedmiot zamówienia (również na dachu budynków). Za każdorazowe złamanie tego zakazu zostanie naliczona kara w wysokości 1 000,00 zł, a pracownik łamiący ten zakaz zostanie wykluczony z dalszych prac. Ponadto jeżeli palenie tytoniu lub używanie substancji wonnych spowoduje reakcję systemu detekcji pożaru w budynku Zamawiającego, co może doprowadzić do wyzwolenie systemu gaszenia, to Wykonawca zobowiązany jest do pokrycia wszystkich wynikłych z tego zdarzenia kosztów.
10) Zabronione jest spożywanie posiłków i napojów w salach komputerowych.
11) Wywóz odpadów z dostaw sprzętu musi odbywać się sukcesywnie w czasie dostawy. Zabronione jest korzystanie z kontenerów Zamawiającego. Wykonawca zobowiązany jest do wywozu całości odpadów na swój koszt i swoimi siłami. Dozwolone jest posadowienie dodatkowego kontenera przy budynku o pojemności nie większej niż

1,7 m3 chyba, że na etapie realizacji zostanie to ustalone inaczej. Za każdy rozpoczęty metr sześcienny pozostawianych odpadów zostanie naliczona kara umowna w wysokości 2 000,00 zł. Warunkiem podpisania protokołu zdawczo - odbiorczego przedmiotu zamówienia jest usunięcie wszystkich odpadów powstałych w trakcie instalacji.

12) Wszystkie prace instalacyjne muszą być wykonane w oparciu o najlepsze praktyki, standardy, najnowszą wiedzę w zakresie który obejmuje zamówienie oraz obowiązujące przepisy.

10.2.2. Warunki instalacji zapewnione przez Zamawiającego

1) Miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu wyposażonym m.in. w podłogę techniczną z szachtami technicznymi na potrzeby prowadzenia okablowania pomiędzy szafami, klimatyzację, system kontroli dostępu i monitoring.
2) Jeden kiosk składający się z 16 szaf teletechniczny.
3) Każda z szaf teletechnicznych posiada wymiary:
   i. wysokość 47U,
   ii. szerokość 80cm,
   iii. głębokość 120cm,
   iv. nośność szafy 1500kg,
   v. nośność belek/profili nośnych (pionowych) 1500kg,
   vi. odległość między belkami umożliwiająca montaż urządzeń z uchwytami w rozstawie 19”.
4) W każdej z szaf zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU.
5) Każda z listew PDU posiada:
   i. zasilanie 3 fazowe,
   ii. zabezpieczenie o łącznej mocy 32A na każdą szafę,
   iii. 18 gniazd C13,
   iv. 6 gniazd C19.
6) Sumaryczne chłodzenie na cały kiosk o mocy 200kW, realizowane za pomocą klimatyzatorów międzyrzędowych.
7) W kiosku znajduje się dedykowany łącznik z włóknami światłowodowymi na potrzeby komunikacji z infrastrukturą Zamawiającego (na potrzeby dostępu do infrastruktury Zamawiającego oraz systemu zdalnego) – parametry łącznika:
   i. złącza SC/APC;
   ii. włókna SM w kablu to G.652d firmy Corning E9/125 SMF-28e+

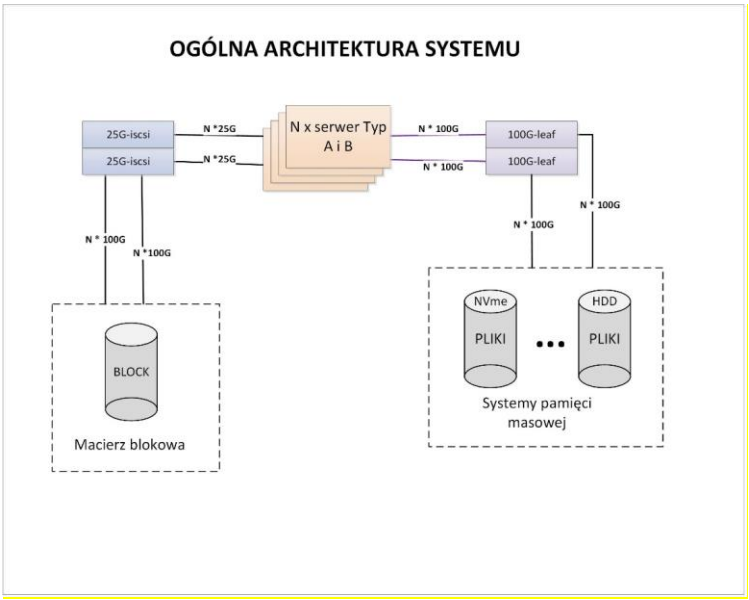
10.2.3. Szczegółowe wymagania dotyczące dostawy i instalacji, które musi spełnić Wykonawca

1) Dostarczenie wszystkich niezbędnych elementów (urządzeń, okablowania, elementów montażowych itp.,) potrzebnych do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną.
2) Wykonanie infrastruktury teletechnicznej z wykorzystaniem:

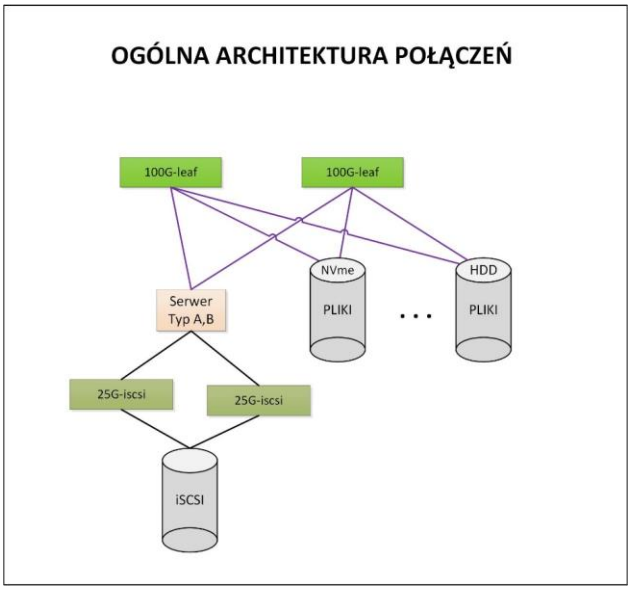
   i. dla połączeń Out-of-Band z wykorzystaniem okablowania miedzianego kategorii min. 6,
   ii. dla pozostałych połączeń z wykorzystaniem okablowania światłowodowego – patchordy dupleksowe (dwa włókna), jednomodowe lub wielomodowe, złącze typu LC,
   iii. Zamawiający nie dopuszcza możliwości stosowania kabli typy „DAC" (ang. Direct Attach Cable),
   iv. Zamawiający nie dopuszcza stosowania kabli typu „breakout".
3) Wykonanie osobnej dedykowanej (odseparowanej fizycznie i logicznie) infrastruktury sieciowej (zgodnie z zaakceptowaną Dokumentacją Techniczną) na potrzeby:
   i. dostępu do dostarczonych zasobów serwerowych, platformy wirtualizacyjnej, systemu pamięci masowych,
   ii. dostępu do systemu przestrzeni dyskowej z dostarczonych serwerów realizowanej za pomocą protokołu iSCSI lub NVMe Over TCP,
   iii. zarządzania dostarczoną infrastrukturą Out-of-Band wszystkich dostarczonych urządzeń posiadających taką funkcjonalność.
4) Zamawiający przewiduje następujące kategorie przełączników sieciowych podzielone wg. ich przeznaczenia, które nie będą ze sobą współdzielone:
   i. „1G-mgmt" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) iii.**
   ii. „25G-iscsi" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) ii.**
   iii. „100G-leaf" – na potrzeby realizacji infrastruktury sieciowej opisanej w ustępie **3) i**., przełączniki, do których muszą być podłączone tylko dostarczone serwery oraz dostarczone systemy pamięci masowej,
5) Każda z podanych w ustępie **3)** infrastruktur musi zostać wykonana za pomocą osobnych i przeznaczonych tylko do jej realizacji urządzeń sieciowych oraz dedykowanego dla niej okablowania teletechnicznego.
6) Infrastruktura podana w ustępie **3) i.** musi zostać zrealizowana w technologii EVPN-VXLAN w architekturze „leaf and spine".
7) Dostarczone serwery na potrzeby realizacji infrastruktury opisanej w ustępie **3) i.** muszą zostać podłączone do dedykowanych dla nich przełączników sieciowych w sposób zapewniający optymalne wykorzystanie infrastruktury sieciowej, nie powodujący generowania zbędnego ruchu pomiędzy przełącznikami, tj.:
   i. interfejsy dostępowe (100G) serwerów **Typu A i B** należy podłączyć do tej samej pary przełączników typu „100G-leaf" w topologii „leaf and spine",
8) Dostarczone serwery oraz macierze blokowe, na potrzeby realizacji infrastruktury opisanej w ustępie **3) ii.** muszą zostać podłączone w sposób redundantny do dedykowanych tylko do tego celu przełączników sieciowych typu „25G-iscsi".
9) Dostarczone systemy pamięci masowej muszą zostać podłączone wszystkimi dostępnymi interfejsami typu „front-end" oraz w sposób zapewniający optymalne wykorzystanie infrastruktury sieciowej, nie powodujący generowania zbędnego ruchu pomiędzy przełącznikami, tj.:

i. interfejsy dostępowe (100G) systemu szybkiej pamięci masowej o dostępie plikowym należy podłączyć do tej samej pary przełączników typu „100G-leaf" w topologii „leaf and spine",

10) Każdy z przełączników typu „100G-leaf" musi zostać połączony z każdym z przełączników typu „100G-leaf" za pomocą 2 (dwóch) połączeń o przepustowości 100G, każde z wykorzystaniem włókien światłowodowych zgodnie z wymaganiami opisanymi w ustępie 2).
11) Poglądowy schemat wymagań Zamawiającego w zakresie ogólnej architektury systemu (topologii połączeń) przedstawiono na poniższym rysunku:



12) Każde urządzenie podłączone do infrastruktury sieciowej musi być podłączone redundantnie (tj. co najmniej do 2 niezależnych przełączników sieciowych) w celu zapewnienia bezprzerwowego dostępu do urządzenia w przypadku awarii jednego z przełączników do którego podłączone jest to urządzenie – poglądowy schemat wymagań Zamawiającego przedstawiono na poniższym rysunku:



13) Każdy z przełączników służących do realizacji infrastruktury opisanej w ustępie **3) i.** oprócz wkładek służących do realizacji tej infrastruktury musi zostać wyposażony w dodatkowe, nie wykorzystane do połączeń, 4 (cztery) wkładki typu 100G-SR4 lub kompatybilne, zgodne i poprawnie pracujące z zaoferowanymi przełącznikami.
14) Wymaga się by wszystkie dostarczone moduły mogły być instalowane w urządzeniu i wyjmowane z urządzenia podczas jego pracy (ang. Hot-Pluggable).
15) Wykonanie wszystkich niezbędnych połączeń teletechnicznych i elektrycznych na potrzeby instalacji dostarczonych urządzeń, w tym także wszystkich wymaganych przewodów ochronnych.
16) Wszystkie dostarczone urządzenia oraz elementy infrastruktury teletechnicznej i elektrycznej muszą być jednoznacznie oznaczone zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
17) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz.
18) Wszystkie połączenia muszą być prowadzone w zgodnie z obowiązującymi normami oraz wytycznymi producentów. Wszystkie połączenia prowadzone pomiędzy szafami muszą być ułożone pod podłogą techniczną. Wszystkie połączenia prowadzone wewnątrz szaf muszą być ułożone w dedykowanych do tego celu uchwytach oraz w sposób umożliwiający przeprowadzenie prac serwisowych na dostarczonych urządzeniach. W tym celu należy wykorzystać m.in. ramiona i uchwyty/organizery do prowadzenia okablowania. Okablowanie musi być ułożone w sposób estetyczny.

19) Wszystkie dostarczone elementy okablowania muszą być jednoznacznie oznaczone w sposób uzgodniony z Zamawiającym, zgodnie z uzgodnionym z Zamawiającym schematem nazewnictwa.
20) Adresacja IP musi zostać zaplanowana w uzgodnieniu z Zamawiającym dla każdego z urządzeń i segmentów sieci.
21) Zaplanowanie i wykonanie dedykowanej infrastruktury zarządzania Out of Band (**3) iii.**) przy użyciu przełączników typu „1G-mgmt". Każdy rodzaj urządzeń na potrzeby zdalnego dostępu Out of Band musi posiadać oddzielną adresację IP (adresacja musi zostać uzgodniona z Zamawiającym na etapie planowania).
22) Wykonania integracji wdrożonego Systemu, w szczególności platformy wirtualizacyjnej, systemu pamięci masowej, infrastruktury dostępowej (zdefiniowanej w ustępie **3) i.**) oraz zarządzania (zdefiniowanej w ustępie **3) iii.**) z infrastrukturą Zamawiającego zainstalowaną w siedzibie Zamawiającego (uzgodnienie adresacji, dostarczenie i ułożenie okablowania). Należy wykonać integrację następujących segmentów:
    i. dostępu do dostarczonych zasobów serwerowych i pamięci masowych z Internetu przy pomocy dwóch redundantnych podłączeń z wykorzystaniem przełączników typu „100G-leaf"

    Integrację należy dokonać z wykorzystaniem łącznika opisanego w punkcie **10.2.2.** Na potrzeby integracji należy dostarczyć patchordy zgodnie z wytycznymi z ustępu **2)** oraz informacjami nt. złącz łącznika opisanych w u punkcie **10.2.2.** Łączna długość każdego połączenia nie przekroczy 2 km.
23) Dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji wdrożenia Systemu zgodnie z zapisami SWZ i Dokumentacją Techniczną.
24) Wykonanie wszystkich niezbędnych połączeń, w tym także podłączeń przewodów ochronnych.
25) Wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
26) Wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
27) Wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz.
28) Przełączniki sieciowe muszą być zainstalowane na tyle szafy patrząc od zewnątrz kiosku i przepływ powietrza musi odbywać się w kierunku od tył urządzenia do frontu (porty we/wy).
29) Dostarczone oprogramowanie do wirtualizacji wraz z modułami oraz oprogramowaniem do wykonywania kopii zapasowych musi zostać zainstalowane na wszystkich dostarczonych serwerach i skonfigurowane zgodnie z wykonaną przez Wykonawcę na podstawie wytycznych Zamawiającego Dokumentacją Techniczną.
30) Macierze blokowe, systemy pamięci masowej muszą zostać zainstalowane, skonfigurowane zgodnie z wykonaną przez Wykonawcę i zaakceptowaną przez Zamawiającego Dokumentacją Techniczną.

31) Wykonanie wszystkich pozostałych czynności zawartych w niniejszym dokumencie oraz znajdujących się w wykonanej przez Wykonawcę i zaakceptowanej przez Zamawiającego Dokumentacji Technicznej.
32) Jeżeli instalowane oprogramowanie lub dostarczany Komponent wymaga przypisania licencji do świadczenia wymaganej funkcjonalności licencja ta musi zostać przypisana oraz aktywowana.

10.3. Dokumentacja

1) Przygotowane przez Wykonawcę, w terminach wynikających ze planu wdrożenia opisanego w punkcie **10.1**, dokumenty:

   a) Dokumentacja Techniczna,
   b) plany testów zgodnie z wytycznymi opisanymi w punkcie **10.6**,
   c) Dokumentacja Powykonawcza

   podlegają akceptacji Zamawiającego.
2) Zamawiający może zgłosić uwagi do dokumentów, o których mowa w ust. 1 powyżej, w terminach podanych w punkcie z **10.1** od ich otrzymania.
3) W przypadku zgłoszenia przez Zamawiającego uwag i zastrzeżeń do dokumentów, o których mowa w ust. 1 powyżej, Wykonawca zobowiązany jest ustosunkować się do stanowiska Zamawiającego nie później niż w terminie podanym w punkcie z **10.1**, od dnia zgłoszenia uwag, natomiast Zamawiający nie później niż w terminie podanym w punkcie **10.1**, od otrzymania odpowiedzi Wykonawcy, o której mowa powyżej, wypowiada się co do akceptacji poprawionej wersji dokumentu. Wykonawca zobowiązany jest do wprowadzenia wszystkich uwag i zastrzeżeń zgłoszonych przez Zamawiającego w terminach podanych w punkcie z **10.1** od ich otrzymania.
4) W celu uniknięcia wątpliwości strony ustalają, że zaakceptowanie przez Zamawiającego dokumentów, o których mowa w ust. 1 powyżej, nie zwalnia Wykonawcy z odpowiedzialności za spełnienie funkcjonalności określonych w SWZ.
5) Szczegółowe wytyczne dla dokumentacji zostały wskazane punktach **10.4** i **10.5**.
6) Szczegółowe wytyczne dla testów zostały wskazane punkcie **10.6**.

10.4. Dokumentacja Techniczna

Przed przystąpieniem do realizacji dostawy przez Wykonawcę musi zostać zaakceptowana przez Zamawiającego Dokumentacja Techniczna w celu weryfikacji poprawności koncepcji realizacji przedmiotu zamówienia z wymaganiami Zamawiającego. Dokumentacja techniczna musi spełniać następujące wymagania:

1) musi być oparta o najlepsze praktyki, standardy i najnowszą wiedzę w zakresie który obejmuje,
2) musi zostać zaakceptowana przez Zamawiającego przed rozpoczęciem dostaw,
3) musi zawierać co najmniej:
   a) listę wymagań funkcjonalnych Zamawiającego,
   b) sposób realizacji wymagań funkcjonalnych,
   c) architekturę Systemu,
   d) fizyczny i logiczny model połączeń poszczególnych Komponentów,

e) architekturę platformy wirtualizacyjnej zbudowanej na bazie dostarczanego oprogramowania do wirtualizacji wraz z modułami opisanego w punkcie **7**,
f) architekturę systemu przestrzeni dyskowej zbudowanego na bazie dostarczonej macierzy blokowej opisanej w punkcie **3**,
g) architekturę systemu pamięci masowej zbudowanego na bazie dostarczonych systemów pamięci masowej opisanych w punktach **4** i **5**,
h) architekturę połączeń elementów sieciowych na potrzeby realizacji poszczególnych funkcjonalności (dostęp do systemów pamięci masowej z serwerów, dostęp do Internetu z serwerów, zdalny dostęp, zarządzanie Out of Band, itd.)
i) architekturę połączeń wszystkich elementów sieciowych (co najmniej: adresacja IP, diagramy połączeń, sposób realizacji redundancji połączeń pomiędzy urządzeniami),
j) architekturę systemu do wykonywania kopii zapasowych przy użyciu dostarczonego oprogramowania do wykonywania kopii zapasowych opisanego w punkcie **6**,
k) aranżację poszczególnych elementów w szafach teletechnicznych,
l) schemat nazewnictwa wszystkich dostarczonych elementów,
m) schemat nazewnictwa wszystkich wykorzystywanych interfejsów,
n) plany konfiguracji sieci w tym adresacji, portów itd. (IP design) wszystkich podłączonych do sieci Komponentów,
o) plany instalacji urządzeń i podłączenia do sieci LAN i zasilania, w tym porty itd. (obwody prądowe),
p) opis integracji, a w tym:
    i. architektura i sposób zapewnienia zdalnego dostępu do poszczególnych Komponentów,
q) listę wdrażanych Komponentów wraz z ich ilościami,
r) szczegółowy wykaz dostarczonych licencji na oprogramowanie,
s) dokumentacje producenckie wszystkich użytych Komponentów i elementów systemu (może być dostarczona w wersji elektronicznej),
t) inne, wg uznania Wykonawcy.

10.5. Dokumentacja Powykonawcza

Dokumentacja Powykonawcza musi spełniać poniższe wymagania.

1) Dokumentacja Powykonawcza musi być opracowana na podstawie założeń zapisanych w Dokumentacji Technicznej (opisanej w punkcie **10.4**) i jeśli od niego odbiega powinien być załączony opis z czego ta różnica wynika
2) Dokumentacja Powykonawcza musi zawierać szczegółowe procedury eksploatacyjne i utrzymaniowe, a także procedury zgłaszania do Wykonawcy awarii i problemów z Systemem w okresie gwarancji.
3) Dokumentacja Powykonawcza musi zawierać szczegółową konfigurację dostępów administracyjnych do Komponentów.
4) Dokumentacja Powykonawcza musi zawierać procedury zarządzania użytkownikami i ich uprawnieniami.
5) Dokumentacja Powykonawcza musi zawierać procedury tworzenia kopii zapasowych i odzyskiwania danych z utworzonych kopii.

6) Dokumentacja Powykonawcza musi zawierać dokumentację producentów elementów składowych Komponentów Systemu i dokumentację rozwiązań technologicznych, w postaci elektronicznej oraz dostępu do zasobów elektronicznych producenta na stronie WWW przez okres gwarancji.
7) Dokumentacja Powykonawcza musi także zawierać co najmniej:
   a) listę zainstalowanych urządzeń z numerami seryjnymi, wersją zainstalowanego oprogramowania oraz opis wykonanej instalacji fizycznej,
   b) schemat rozmieszczenia poszczególnych urządzeń w szafach,
   c) zestawienie wykonanych połączeń fizycznych pomiędzy zainstalowanymi urządzeniami na potrzeby sieci, z uwzględnieniem nazw i numerów interfejsów, typów połączeń i oznaczeniem połączeń,
   d) dokumentację infrastruktury sieciowej wybudowanej na potrzeby realizacji wdrożenia – co najmniej: schemat połączeń logicznych i fizycznych, zestawienie użytych adresacji IP, konfiguracja urządzeń sieciowych,
   e) dokumentację zarządzania Out-of-Band dostarczonymi urządzeniami – co najmniej: schemat połączeń logicznych i fizycznych, zestawienie użytych adresacji IP, konfiguracja urządzeń zapewniających dostęp zarządzania Out-of-Band,
   f) dokumentacja fotograficzna wykonanej instalacji,
   g) opis konfiguracji poszczególnych urządzeń,
   h) zestawienie informacji o podłączeniu zainstalowanych urządzeń do zasilania.
8) Procedury administracyjne opisujące czynności dla Systemu muszą zawierać co najmniej następujące opisy:
   a) procedury instalacji poszczególnych Komponentów,
   b) procedury utrzymaniowe,
   c) procedury diagnostyczne w przypadku awarii.
9) Opis architektury systemu obejmujący co najmniej następujące elementy:
   d) szczegółowy model architektury Komponentów rozwiązania wraz z integracjami,
   e) opis scenariuszy i raportów wszystkich testów,
   f) szczegółowa architektura platformy wirtualizacyjnej wraz z jej modułami,
   g) szczegółowa architektura dostarczonych macierzy i systemów pamięci masowej,
   h) szczegółowa architektura bezpieczeństwa Systemu
   i) szczegółowa architektura systemu do wykonywania kopii zapasowych,
   j) opis konfiguracji elementów Systemu zgodnie z wymaganiami z punktu **10.2.3**,
   k) architektura, opis działania oraz parametry HA,
   l) szczegółowa architektura i konfiguracja wszystkich przewidzianych integracji,
   m) szczegółowy opis procedur eksploatacyjnych, utrzymaniowych i awaryjnych Systemu i wszystkich Komponentów wchodzących w skład Systemu,
   n) szczegółowy opis monitorowania, raportowania i automatyzacji Komponentów wchodzących w skład Systemu,
   o) szczegółowy opis i konfiguracja Systemu w zakresie dostępu administracyjnego, uwierzytelniania i autoryzacji dla użytkowników,
   p) instrukcje administratora systemu (co najmniej na poziomie zarządzania i używania, oraz analizy możliwych problemów).

10) Dokumentacja Powykonawcza w zakresie konfiguracji musi obejmować wszystkie elementy wdrożone, zainstalowane w ramach realizacji przedmiotu zamówienia. Minimalny zestaw wymaganych danych konfiguracyjnych obejmuje:
    a) model urządzenia, parametry sprzętowe (np. kontrolery, półki dyskowe, dyski, przełączniki, moduły optyczne, itp.), konfigurację macierzy blokowych i systemów pamięci masowej (grupy dyskowe, zasoby dyskowe itp.), sposób podłączenia wszystkich Komponentów do infrastruktury Zamawiającego,
    b) schemat infrastruktury wraz z opisem,
    c) licencje dla dostarczonych elementów Systemu,
    d) informacje o ograniczeniach technologicznych (liczba dysków, rozmiar cache, itp.) dostarczonych elementów infrastruktury,
    e) procedury utrzymaniowe dla poszczególnych komponentów,
    f) procedury aktualizacji oprogramowania,
    g) procedury zgłaszania problemów,
    h) opracowanie procedur eksploatacyjnych dla pierwszej linii wsparcia: diagnostyka, monitoring, analiza awarii,
    i) opracowanie dokumentacji w zakresie procedur awaryjnych dla pierwszej linii wsparcia, umożliwiających diagnozowanie Systemu i podstawowej weryfikacji przyczyny problemu.
11) Do Dokumentacji Powykonawczej musi być załączony raport z testów wykonanych po realizacji wdrożenia.

10.6. Wytyczne do testów

Proces testowania Systemu związany z wdrożeniem i ewentualnymi zmianami w Systemie składa się następujących działań:

1) przygotowanie Systemu – Wykonawca przygotowuje System do wdrożenia i opracowuje scenariusze testowe oraz zakres testów akceptacyjnych, które muszą być zaakceptowane przez Zamawiającego,
2) testy weryfikacyjne na dostarczonym Systemie – realizowane samodzielnie przez Wykonawcę; ich wyniki nie przesądzają o odbiorze Systemu,
3) testy akceptacyjne – realizowane przez Wykonawcę we współpracy z Zamawiającym, na podstawie wcześniej przygotowanego i zaakceptowanego zakresu testów akceptacyjnych, celem sprawdzenia poprawności przygotowania Systemu,
4) testy wydajnościowe – realizowane przez Wykonawcę we współpracy z Zamawiającym, na podstawie wcześniej przygotowanego i zaakceptowanego zakresu testów wydajnościowych, celem sprawdzenia wydajności Systemu,
5) zaakceptowane wyniki testów – zakończone z sukcesem testy akceptacyjne Systemu,
6) testy odbiorcze – realizowane przez Wykonawcę we współpracy z Zamawiającym, na podstawie zaakceptowanych wcześniej scenariuszy testowych.

10.6.1. Testy weryfikacyjne

Nazwa testów	Testy weryfikacyjne

Cel testów	weryfikacja czy dostarczone i zainstalowane środowisko jest gotowe do pełnienia funkcji produkcyjnej
Realizujący	Wykonawca

Wykonawca samodzielnie przygotowuje zakres, scenariusze testowe, dane testowe i realizuje testy. Po zakończeniu testów Wykonawca jest zobowiązany do dostarczenia Zamawiającemu raportu z realizacji testów.
W zakres testów weryfikacyjnych muszą wchodzić przynajmniej poniższe elementy:

1) testy zdalnego dostępu do Systemu i jego wszystkich elementów,
2) weryfikacja instalacji wszystkich elementów Komponentów Systemu,
3) testowanie składników zarządzania Systemem,
4) testowanie i zatwierdzanie wdrożonego projektu architektury Systemu.

10.6.2. Testy akceptacyjne (podstawowe i niezawodnościowe)

Nazwa testów	Testy akceptacyjne (podstawowe i niezawodnościowe)
Cel testów	weryfikacja poprawności działania poszczególnych elementów Systemu
Realizujący	Wykonawca we współpracy z Zamawiającym
Wejście	Raport z testów weryfikacyjnych
Wyjście	Raport z testów akceptacyjnych (podstawowych i niezawodnościowych)

Celem przeprowadzonych testów jest weryfikacja poprawności działania dostarczonych Komponentów.
Testy akceptacyjne składają się z następujących elementów:

1) testów podstawowych – podstawowy zakres testów zdefiniowany przez Wykonawcę i zaakceptowany przez Zamawiającego, którego celem jest weryfikacja Komponentów Systemu,
2) testów niezawodnościowych.

W ramach procesu testowania należy zrealizować wszystkie testy, pozytywne zakończenie testów każdego typu jest podstawą do zaakceptowania instalacji Systemu.

Testy podstawowe

Podstawowy zakres testów akceptacyjnych musi obejmować weryfikację:

1) poprawności działania,
2) funkcjonalności,
3) poprawnej konfiguracji,
4) możliwości zarządzania

w odniesieniu do wszystkich dostarczonych Komponentów.
Podstawowy zakres testów akceptacyjnych musi obejmować co najmniej poniższe scenariusze:

1) tworzenie maszyn wirtualnych,
2) wykonywanie snapshot-ów maszyn wirtualnych,
3) klonowanie maszyn wirtualnych,
4) migrowanie maszyn między hostami zarówno dla warstwy obliczeniowej jak i danych,

5) przygotowanie infrastruktury do korzystania z programowalnej sieci komputerowej (ang. SDN),
6) tworzenie i zarządzanie logicznymi segmentami sieci,
7) tworzenie i zarządzanie logicznym routingiem,
8) tworzenie i zarządzanie serwisami/usługami logicznymi (dhcp, load balancer, nat),
9) tworzenie i zarządzanie regułami bezpieczeństwa – koncepcja zero trust security,
10) korzystanie z narządzenia do monitorowania i rozwiązywania problemów,
11) weryfikację poprawności konfiguracji klastra i wykorzystania kompatybilnych Komponentów serwera,
12) weryfikacja wszystkich elementów serwera i ich parametrów,
13) weryfikacja możliwości zarzadzania serwerami,
14) weryfikacja wszystkich parametrów macierzy blokowych i systemów pamięci masowej,
15) weryfikacja możliwości zarzadzania macierzami blokowymi i systemami pamięci masowej,
16) weryfikacja wszystkich elementów infrastruktury sieciowej,
17) weryfikacja możliwości zarządzania poszczególnymi elementami infrastruktury sieciowej,
18) weryfikacja poprawności działania usługi zdalnego dostępu do infrastruktury dla administratorów,
19) weryfikacja możliwości zarządzania poszczególnymi elementami systemu za pomocą usługi zdalnego dostępu,
20) wykonanie kopii zapasowej maszyny wirtualnej,
21) odtworzenie maszyny wirtualnej z kopii zapasowej.

Za realizację testów odpowiada Wykonawca, realizując je wspólnie z Zamawiającym. Zakres testów powinien być spójny ze scenariuszami testów odbiorczych, jednakże może zostać zmodyfikowany w trakcie prac projektowych po akceptacji Zamawiającego. Do realizacji testów akceptacyjnych należy przygotować listy funkcjonalności / procesów wymagających przetestowania, nie muszą to być pełne scenariusze testowe.

Zakończenie testów akceptacyjnych jest możliwe po zamknięciu wszystkich zgłoszonych błędów, czy to poprzez ich rozwiązanie, czy poprzez ustalenie pomiędzy Zamawiającym i Wykonawcą, że dany błąd nie jest błędem istotnym.

Testy niezawodnościowe

Zakres testów niezawodnościowych musi obejmować weryfikację możliwych awarii w odniesieniu do wszystkich dostarczonych Komponentów.

Podstawowy zakres testów niezawodnościowych musi obejmować co najmniej poniższe symulacje:

1) symulacje awarii hosta w klastrze z wyłączeniem HA oraz test z włączonym HA dla maszyn wirtualnych z przypisana polityką odporności na awarię minimum jednego hosta,
2) symulacje awarii dysku z danymi w macierzach dyskowych oraz w systemach pamięci masowej,
3) symulacje awarii dysku cache w systemach pamięci masowej,
4) symulacje awarii połączenia sieciowego w serwerze,
5) symulacje awarii przełącznika LAN,
6) wprowadzenie serwera w tryb konserwacji i wyprowadzenie go z tego trybu i obserwacje dostępności wirtualnych maszyn w klastrze,
7) symulacje awarii każdego z Komponentów Systemu dla potwierdzenia pełnej redundancji.

10.6.3. Testy wydajnościowe

Nazwa testów	Testy wydajnościowe
Cel testów	Weryfikacja czy dostarczony System zapewnia wystarczającą wydajność
Realizujący	Wykonawca we współpracy z Zamawiającym
Wejście	Raport z testów akceptacyjnych (podstawowych i niezawodnościowych)
Wyjście	Raport z testów wydajnościowych

Wykonawca jest zobowiązany do przygotowania i przeprowadzenia we współpracy z Zamawiającym testów wydajnościowych, których celem jest weryfikacja, czy System zapewnia odpowiednie parametry zgodnie z wymaganiami zamieszczonymi w opisie technicznym.
Wykonawca jest zobowiązany do przeprowadzenia testów w oparciu o gotowe, istniejące na rynku, narzędzia/programy.
Wynikiem przeprowadzonych testów musi być potwierdzenie parametrów wydajnościowych wymaganych przez Zamawiającego w niniejszym SWZ. Zakres parametrów wydajnościowych musi obejmować co najmniej:

1) w przypadku serwerów – potwierdzenie wydajności w teście CPU2017 Floating Point Rate zgodnie z wymaganiami zawartymi w SWZ,
2) w przypadku elementów sieciowych – przepustowości interfejsów dla ruchu typu IMIX zgodnie z wymaganiami zawartymi w SWZ lub w karcie katalogowej producenta jeśli nie podano w SWZ.

Pozytywne zakończenie testów każdego typu jest podstawą do zaakceptowania instalacji Systemu.

10.6.4. Testy odbiorcze

Nazwa testów	Testy odbiorcze
Cel testów	Weryfikacja poprawności działania wszystkich procesów w ramach dostarczonego Systemu
Realizujący	Wykonawca we współpracy z Zamawiającym
Wejście	Raport z testów akceptacyjnych i niezawodnościowych oraz wydajnościowych
Wyjście	Protokół zdawczo – odbiorczy

Wykonawca w ustalonym harmonogramie i terminie zgłasza Zamawiającemu gotowość Systemu do przeprowadzenia testów odbiorczych.

1) Zgłaszając Zamawiającemu gotowość Systemu do przeprowadzenia testów odbiorczych, Wykonawca zobligowany jest przedstawić raport z przeprowadzonych przez siebie testów potwierdzających gotowość do testów odbiorczych i zgodność Systemu z wymaganiami Zamawiającego.
2) Procedury testów odbiorczych muszą zawierać co najmniej następujące elementy:
   a) wprowadzenie
   b) opis przedmiotu testów
   c) zakres testów – testowane obszary

d) wyłączenia z zakresu
e) podejście do testowania
f) kryteria zaliczenia/niezaliczenia testów
g) kryteria zawieszenia i wznowienia testowania
h) czynności i zadania testowania
i) środowiska testowe
j) harmonogram
k) ryzyka i plany awaryjne
l) zatwierdzenie planu.

W celu weryfikacji poszczególnych funkcjonalności Systemu, Zamawiający określi dodatkowe testy funkcjonalne potwierdzające prawidłowe działanie tych funkcjonalności.
Zamawiający wymaga przeprowadzenia co najmniej następujących testów:

1) dostępności:
   a) odporność na awarie dysku w macierzach blokowych oraz w systemach pamięci masowej: wyjęcie jednego, dwóch dysków,
   b) odporność na awarie klastra: wyłączenie jednego, dwóch serwerów,
2) monitorowania warstwy fizycznej urządzenia Systemu:
   a) symulacja awarii/niedostępności zasilania,
   b) symulacja awarii/niedostępności dysku,
3) mikro-segmentacji ruchu sieciowego dla maszyn wirtualnych, weryfikacji kontroli ruchu w warstwie L3 i L4 w jednym segmencie L2 dla komunikacji IP między dwoma maszynami wirtualnymi
   a) testy realizowane na maszynach wirtualnych umieszczonych na jednym i dwóch serwerach fizycznych,
4) weryfikacji wydajności w komunikacji maszyna wirtualna z maszyną wirtualną:
   a) test wydajnościowy w komunikacji IP między maszynami wirtualnymi,
5) wykonania kopi zapasowej w środowisku:
   a) wykonanie i odtworzenie kopii maszyny wirtualnej
6) dostępności danych dla macierzy blokowej i systemów pamięci masowej:
   a) uruchamianie i zatrzymywanie urządzeń,
   b) symulacja awarii pojedynczego węzła,
   c) symulacja awarii pojedynczego portu LAN,
   d) symulacja awarii pojedynczego dysku,
7) całości Systemu:
   a) symulacja awarii jednego z torów zasilania dla zasilaczy w urządzeniach,
   b) symulacja awarii sieci LAN poprzez wyłączenie portów komunikacyjnych LAN.

10.7. Odbiory

Odbiór oznacza przeprowadzenie testów odbiorczych oraz potwierdzenie protokołem zdawczo – odbiorczym zgodności przedmiotu zamówienia z warunkami umowy.
Protokolarnemu odbiorowi przez Zamawiającego podlegać będą:

1) dostawa sprzętu, oprogramowania i licencji,
2) dokumentacja techniczna,
3) raporty z testów,

4) wykonanie całości odbieranego przedmiotu zamówienia.

11. Gwarancja

11.1. Ogólne warunki Gwarancji

1) Wykonawca zobowiązuje się do udzielenia gwarancji na dostarczone urządzenia, oprogramowanie oraz wykonane prace i zobowiązuje się do wykonywania świadczeń gwarancyjnych zgodnie z poniższymi warunkami.
2) Okres gwarancji na System wynosi 7 (siedem) lat i rozpoczyna swój bieg od daty podpisania protokołu zdawczo-odbiorczego. Zamawiający dopuszcza, aby okres gwarancji na dostarczone stacje zarządzania był krótszy, jednak w takim przypadku musi być on zgodny z minimalnymi warunkami opisanym w punkcie **11.2.15.**
3) Zamawiający może dokonać rozbudowy posiadanej infrastruktury sprzętowej, aplikacyjnej oraz teleinformatycznej wchodzącej w skład Systemu, bez utraty uprawnień wynikających z gwarancji na dostarczony i wdrożony System w ramach realizacji przedmiotu zamówienia, z zastrzeżeniem, że rozbudowa została dokonana zgodnie z zaleceniami/wytycznymi producenta/producentów rozbudowywanych elementów Systemu.
4) Gwarancja nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów urządzeń i/lub oprogramowania.
5) Wykonywanie praw wynikających z udzielonej gwarancji nie wyłącza wykonywania uprawnień Zamawiającego wynikających z rękojmi za wady urządzeń i/lub oprogramowania. Zamawiający jest uprawniony do wykonywania uprawnień wynikających z rękojmi na warunkach analogicznych jak realizacja uprawnień Zamawiającego wynikających z gwarancji.
6) W ramach gwarancji Wykonawca zobowiązany jest do:
    a) diagnostyki i rozwiązywania problemów zgłaszanych przez Zamawiającego,
    b) wsparcia w zakresie dostarczonego oprogramowania poprzez zapewnienie:
        i. dostępu do poprawek (aktualizacji) oprogramowania, w szczególności poprzez udostępnienie odpowiednich haseł, kodów, itp. narzędzi do systemów serwisowych producentów lub dostawców,
        ii. zapewnienie dostępu do najnowszych komercyjnie dostępnych wersji oprogramowania wraz z zapewnieniem niezbędnych licencji na warunkach nie gorszych niż wynikających z SWZ, i to bez dodatkowych kosztów dla Zamawiającego, w szczególności poprzez udostępnienie odpowiednich haseł, kodów, itp. narzędzi do systemów serwisowych producentów lub dostawców,
    c) udzielania konsultacji dotyczących instalacji, funkcjonowania i aktualizacji Systemu,
    d) dostarczenia urządzeń oraz oprogramowania wolnego od wad materiałowych i wykonawczych w trakcie okresu świadczenia usług gwarancji,
    e) w okresie gwarancji Wykonawca będzie udostępniał Zamawiającemu dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej oprogramowania i urządzeń,
    f) gwarancja na urządzenia i oprogramowanie będzie świadczona w miejscu używania urządzeń i oprogramowania z możliwością naprawy w serwisie Wykonawcy po uzyskaniu zgody Zamawiającego,
    g) wszelkie koszty rozwiązywania problemów, w tym koszt transportu, instalacji i uruchomienia urządzeń i oprogramowania ponosi Wykonawca,

h) Wykonawca i Zamawiający będą współpracować przy rozwiązywaniu problemów,
i) Wykonawca zapewni naprawę lub wymianę Komponentów lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta urządzeń. Zamawiający w uzasadnionych przypadkach ma prawo wnioskować do Wykonawcy o oficjalne potwierdzenie zgodności przeprowadzonych prac z metodyką i zaleceniami producenta, które musi być wystawione przez producenta urządzeń lub podmiot do tego uprawniony, a Wykonawca w ciągu 14 dni dostarczy takie potwierdzenie Zamawiającemu,
j) dokonania wymiany Komponentu w okresie gwarancji na nowy w przypadku 3 (trzech) istotnych jego awarii; za istotną awarię uznaje się każde uszkodzenie ograniczające funkcjonowanie przedmiotu zamówienia; wymiana przedmiotu zamówienia powinna nastąpić w terminach nie dłuższych niż czas dostawy; w przypadku wymiany uszkodzonego asortymentu (albo jego podzespołu) na nowy obowiązywać będą warunki gwarancji i realizacji świadczeń gwarancyjnych wynikające ze złożonej oferty; okres gwarancji będzie biegł w takim przypadku od początku,
k) dla dostarczonego sprzętu przez cały okres trwania gwarancji musi być zapewniona możliwość aktualizacji oprogramowania/firmware do najnowszej dostępnej wersji producenta. Koszty aktualizacji ponosi Wykonawca.
l) dostarczony przedmiot zamówienia musi być fabrycznie nowy, nieeksponowany na wystawach, kompletny i sprawny technicznie. Przez stwierdzenie „fabrycznie nowy" należy rozumieć przedmiot zamówienia oryginalnie zapakowany, nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testu jego poprawnej pracy po wyprodukowaniu,
m) dostarczony przedmiot zamówienia musi pochodzić z oficjalnych kanałów dystrybucyjnych producenta niewyłączających sprzedaży na rynku polskim zapewniających w szczególności realizację uprawnień gwarancyjnych,
n) W przypadku, gdy Wykonawca podczas realizacji usług gwarancyjnych dostarczy nową fabrycznie część Komponentu, wymieniając część wadliwą, lub dostarczy fabrycznie nowe urządzenie, nowa część lub nowe urządzenie staje się własnością Zamawiającego,
o) Zamawiający może dokonać rozbudowy Systemu bez utraty uprawnień wynikających z gwarancji na urządzenia i oprogramowanie,
p) Wykonawca zapewni zdalne wsparcie (poprzez platformę do współpracy, telefon lub e-mail) w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania.

11.2. Opis usługi Gwarancji

11.2.1. Diagnostyka i rozwiązywanie problemów

W zakresie gwarancji Wykonawca zapewnia Zamawiającemu usługę diagnostyki i rozwiązywania problemów w ramach Systemu.

11.2.2. Klasyfikacja problemów

Klasyfikację problemów określa Zamawiający. W przypadku, gdy strony zgodzą się, że System pomimo zgłoszenia funkcjonuje prawidłowo, zgłoszenie to nie jest uznawane za awarię.
Awaria Krytyczna – wystąpienie problemu o znaczeniu krytycznym dla Zamawiającego, powodujące poważne i szkodliwe zakłócenie działania Systemu. W szczególności możliwe są problemy z bezpieczeństwem, naruszenia zgodności, straty i szkody dla reputacji. Spełniona zostaje co najmniej jedna z wymienionych niżej przesłanek:

1) nie jest możliwe korzystanie przez Zamawiającego z Systemu lub korzystanie z niego jest znacząco utrudnione (degradacja),
2) nie działają funkcje Systemu lub występuje ich znacząca degradacja,
3) wydajność lub pojemność Systemu uległa obniżeniu, o co najmniej 40% w stosunku do wartości dostarczonej,
4) nie jest możliwe stwierdzenie stanu Systemu lub jego elementów,
5) brak możliwości realizacji usług.

Awaria Poważna – wystąpienie Problemu, w którym występuje zakłócenie usługi i/lub operacji. Konsekwencje obejmują w szczególności naruszenia zgodności, szkody dla reputacji i możliwe obawy dotyczące bezpieczeństwa. Możliwe są straty. Spełniona zostaje co najmniej jedna z wymienionych niżej przesłanek:

1) brak możliwości zarządzania elementami Systemu,
2) wydajność lub pojemność Systemu uległa obniżeniu, o co najmniej 20% w stosunku do wartości dostarczonej.

Awaria Istotna – wystąpienie Problemu, w wyniku którego powstają utrudnienia w dostępie do komponentu/ów. Obejmuje przerwy w obsłudze użytkownika, głównie o ograniczonym zakresie, czasie trwania lub skutku. Spełniona zostaje co najmniej jedna z wymienionych niżej przesłanek:

1) uszkodzenie komponentu lub jego elementów powodujące ograniczenie możliwości działania Systemu, ale nieuniemożliwiające korzystania z Systemu,
2) stan Systemu, w którym część Systemu nie funkcjonuje zgodnie z dokumentacją aktualnie eksploatowanej wersji Systemu, co utrudnia pracę co najmniej jednej z jego funkcji.

Usterka – pozostałe Problemy.

11.2.3. Poziomy świadczenia usługi

W zależności od klasyfikacji Problemu, Wykonawca gwarantuje następujący czas realizacji Zgłoszeń Zamawiającego:

Klasa Problemu	Maksymalny czas reakcji na zgłoszenie	Maksymalny czas Rozwiązania Problemu[1] (przywrócenia normalnego	Maksymalny czas dostarczenia rozwiązania docelowego[2]	Tryb Serwisowania (godzin na dobę

		działania Systemu)		x liczbę dni w tygodniu)
Awaria Krytyczna	8 godzin	8 godzin	10 dni roboczych	24x7
Awaria Poważna	24 godziny	8 godzin	20 dni roboczych	24x7
Awaria Istotna	24 godziny	16 godzin	80 dni roboczych	8x5[3]
Usterka	24 godziny	40 godzin	100 dni roboczych	8x5[3]

Maksymalny czas reakcji na zgłoszenie	Maksymalny czas dostarczenia rozwiązania docelowego[2]	
	Maksymalny czas Rozwiązania Problemu[1] (przywrócenia normalnego działania)	

Powyższy diagram przedstawia zależność poszczególnych czasów obsługi zgłoszenia – czas rozwiązania problemu i/lub czas na dostarczenie rozwiązania docelowego nalicza się od momentu zakończenia czasu reakcji na zgłoszenie.

[1] – również zastosowanie obejścia, tj. rozwiązania pozwalającego na prawidłowe korzystanie z Systemu bez usuwania wykrytego błędu
[2] – w przypadku zastosowania obejścia
[3] – należy to rozumieć jako tylko w dni robocze

11.2.4. Wymiana informacji pomiędzy Zamawiającym a Wykonawcą

1) Strony dopuszczają następujące kanały komunikacyjne:
   a) system zgłoszeń problemowych Wykonawcy,
   b) poczta elektroniczna,
   c) strona WWW,
   d) systemy VC,
   e) telefon.
2) Zgłoszenia kierowane przez Zamawiającego za pośrednictwem telefonu, będą również potwierdzane niezwłocznie, poprzez wysłanie e-mail do Wykonawcy, z podaniem czasu zgłoszenia za pośrednictwem telefonu. W takiej sytuacji za czas Zgłoszenia Problemu, uważa się moment zgłoszenia za pośrednictwem telefonu.
3) Wykonawca zobowiązany jest przyjmować i rejestrować Zgłoszenia Problemów składane przez Zamawiającego w trybie 24/7/365.

4) Wykonawca będzie aktualizował wszelkie dane o Problemie takie jak postępy prac, statusy, priorytet, typ w systemie zgłoszeń problemowych, a cała historia korespondencji oraz statusów będzie dostępna dla Zamawiającego.
5) Wszelka korespondencja między stronami będzie odbywała się w języku polskim.
6) Szczegóły przekazania dostępów do systemu zgłoszeń problemowych Wykonawcy zostaną przekazane Zamawiającemu w trybie roboczym.
7) Strony, w trakcie trwania usługi gwarancji, mogą umówić się na integracje między systemami zgłoszeń problemowych Wykonawcy i Zamawiającego. Szczegóły zostaną uzgodnione w trybie roboczym.

11.2.5. Zgłaszanie problemów

1) Zamawiający jest odpowiedzialny za przekazanie w zgłoszeniu problemu kompletu znanych mu informacji, w szczególności:
   a) osobę lub osoby kontaktowe reprezentujące Zamawiającego,
   b) identyfikację i lokalizację urządzenia,
   c) opis problemu,
   d) klasyfikację problemu.
2) Za czas zgłoszenia problemu uznaje się moment skutecznego poinformowania Wykonawcy przez Zamawiającego o zaistniałym problemie.
3) Za klasyfikację problemu odpowiedzialny jest Zamawiający.
4) Wykonawca w trybie roboczym będzie przedstawiał swoje uwagi, gdy problemy będą zgłaszane w sposób nieprawidłowy po rozwiązaniu problemu.

11.2.6. Czas reakcji

1) Oznacza czas, który upłynie od wysłania zgłoszenia awarii do podjęcia czynności naprawczych ze strony Wykonawcy.
2) Wykonawca informuje Zamawiającego o przyjęciu zgłoszenia problemu za pośrednictwem poczty elektronicznej lub umieszczeniu odpowiedniej informacji w systemie zgłoszeń problemowych udostępnionym Zamawiającemu.

11.2.7. Rozwiązanie problemu

1) W ramach rozwiązywania problemu Wykonawca prowadzi diagnostykę, mającą na celu znalezienie przyczyn wystąpienia problemu. Diagnostyka będzie prowadzona w miejscu instalacji lub zdalnie po wyrażeniu zgody przez Zamawiającego i udostępnieniu Wykonawcy dostępu do Systemu.
2) Wykonawca informuje Zamawiającego o stanie prac mających na celu rozwiązanie problemu.
3) W przypadku uszkodzenia urządzeń, urządzenia lub części urządzenia, Wykonawca zapewnia dostawę i wymianę uszkodzonych urządzeń, urządzenia lub części urządzenia zgodnie z warunkami opisanymi w niniejszym załączniku. W przypadku, gdy wymienione urządzenia, urządzenie lub część urządzenia wymagają konfiguracji, będzie ona wykonana przez Wykonawcę.
4) Zamawiający po uzgodnieniu z Wykonawcą, ma prawo wymienić uszkodzoną część we własnym zakresie, którą następnie przekaże Wykonawcy w celu naprawy lub wymiany.

5) W przypadku wystąpienia problemu z oprogramowaniem, Wykonawca będzie współpracował z producentem oprogramowania w celu rozwiązania problemu.
6) Rozwiązanie problemu zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt rozwiązania problemu, a Zamawiający ten fakt potwierdzi. Zamawiający zostanie poinformowany o fakcie rozwiązania problemu.

11.2.8. Czas rozwiązania problemu

1) Czas rozwiązania problemu liczony jest oddzielnie dla każdego zgłoszenia problemu.
2) Czas rozwiązania problemu liczony jest od momentu zgłoszenia problemu do momentu poinformowania Zamawiającego przez Wykonawcę o rozwiązaniu problemu.
3) Czas potwierdzenia przez Zamawiającego do Wykonawcy rozwiązania problemu nie liczy się do czasu rozwiązania problemu – na ten czas Wykonawca zawiesza zgłoszenie problemu.
4) W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku rozwiązania problemu, tj. dalszego występowania problemu, Wykonawca odwiesza zgłoszenie problemu i czas rozwiązania problemu jest kontynuowany o czas oczekiwania na dostęp do urządzeń.
5) Jeżeli Wykonawca uchybi terminowi rozwiązania problemu, wskazanemu w punkcie **11.2.3**, z przyczyn leżących po jego stronie, Zamawiający będzie miał prawo do rozwiązania problemu samodzielnie lub poprzez zlecenie innemu podmiotowi przez siebie wybranemu. Takie zastępcze rozwiązanie problemu jest dokonywane na koszt i ryzyko Wykonawcy

11.2.9. Przywrócenie systemu

1) Rozwiązanie problemu polega na przywróceniu normalnego funkcjonowania Systemu za pomocą rozwiązania docelowego.
2) W ramach tymczasowego rozwiązywania Problemu, Wykonawca może zaproponować Zamawiającemu Przywrócenie Systemu poprzez wykorzystanie Obejścia. W takim wypadku maksymalny czas dostarczenia rozwiązania docelowego wydłuża się do czasu wskazanego w kolumnie 4 tabeli zamieszczonej w punkcie **11.2.3**
3) Wykonawca informuje Zamawiającego o stanie prac mających na celu Przywrócenie Systemu.
4) Przywrócenie Systemu z wykorzystaniem Obejścia nie zwalnia Wykonawcy z obowiązku Rozwiązania Problemu, zgodnie z czasami określonymi w niniejszym Załączniku.
5) W przypadku wystąpienia Problemu z Oprogramowaniem, Wykonawca będzie współpracował z producentem Oprogramowania w celu Rozwiązania Problemu.
6) Przywrócenie Systemu zostaje uznane za skuteczne w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt Przywrócenia Systemu, a Zamawiający ten fakt potwierdzi.

11.2.10. Czas przywrócenia systemu

1) Czas przywrócenia systemu mierzony jest oddzielnie dla każdego zgłoszenia problemu.
2) Czas przywrócenia systemu liczony jest od momentu zgłoszenia problemu do momentu poinformowania Zamawiającego przez Wykonawcę o przywróceniu systemu.
3) Czas potwierdzenia przez Zamawiającego do Wykonawcy przywrócenia systemu nie liczy się do czasu przywrócenia systemu – na ten czas Wykonawca zawiesza zgłoszenie problemu.

4) W przypadku skierowania przez Zamawiającego do Wykonawcy informacji o braku przywrócenia Systemu, tj. dalszego występowania problemu, Wykonawca odwiesza zgłoszenie problemu i czas przywrócenia Systemu jest kontynuowany.
5) W przypadku, gdy w celu przywrócenia systemu występuje konieczność wymiany lub naprawy urządzeń, na czas wymiany lub naprawy urządzeń, Zamawiający ma obowiązek zapewnić dostęp do Urządzeń upoważnionym pracownikom Wykonawcy. W przypadku braku takiego dostępu, czas przywrócenia systemu odpowiednio wydłuża się o czas oczekiwania na dostęp do urządzeń.
6) Zgłoszenie problemu po przywróceniu Systemu zostaje ustawione w odpowiedni stan ze stosowną adnotacją, do momentu ostatecznego rozwiązania problemu, zgodnie z czasami określonymi w punkcie **11.2.3**.

11.2.11. Rozwiązanie zgłoszenia problemu

1) Zgłoszenie problemu zostaje uznane za rozwiązane w przypadku, gdy Wykonawca zgłosi Zamawiającemu fakt rozwiązania problemu, a Zamawiający ten fakt potwierdzi.
2) Zamawiający zostanie poinformowany o fakcie rozwiązania problemu za pomocą jednego ze środków komunikacji opisanych w punkcie **11.2.4**, przy czym Wykonawca jednocześnie dokona stosownej adnotacji w systemie zgłoszeń problemowych.
3) Po potwierdzeniu przez Zamawiającego rozwiązania problemu, Wykonawca zamyka zgłoszenie problemu w systemie zgłoszeń problemowych.
4) W przypadku analogicznego zgłoszenia problemu, zostanie ono zarejestrowane przez Wykonawcę pod innym numerem zgłoszenia.

11.2.12. Konsultacje

W zakresie gwarancji Wykonawca zapewnia Zamawiającemu usługę konsultacji.

1) Przedmiot konsultacji:
   a) w zakresie usługi konsultacji, Wykonawca zapewnia Zamawiającemu dostęp do pomocy technicznej Wykonawcy, jako wsparcie w rozwiązywaniu problemów związanych z bieżącą eksploatacją Systemu, w szczególności w zakresie:
      i) obsługi, administracji i konfiguracji urządzeń
      ii) obsługi, administracji i konfiguracji oprogramowania
      iii) wsparcia w rozwiązywaniu problemów u Zamawiającego, które nie są Problemami w rozumieniu zapisów punktu **11**,
   b) osoby świadczące pomoc techniczną po stronie Wykonawcy muszą posiadać odpowiednią wiedzę fachową niezbędną do świadczenia usług konsultacji.

2) Przebieg konsultacji:
   a) Zamawiający kontaktuje się z Wykonawcą drogą mailową lub telefoniczną z opisem sytuacji wymagającej konsultacji,
   b) Wykonawca przekazuje Zamawiającemu potwierdzenie przyjęcia zgłoszenia i rozpoczęcia prac w zakresie danej Konsultacji, zgodnie z czasem podjęcia konsultacji,
   c) strony komunikują się wzajemnie w ramach godzin świadczenia konsultacji,

d) strony dopuszczają zmianę kanału komunikacji na ustalony wspólnie w trybie roboczym,
e) Wykonawca rejestruje usługi konsultacji w celach raportowych.

3) Poziom świadczenia usługi

Wykonawca gwarantuje następujący poziom świadczenia usługi:

Godziny świadczenia konsultacji:	Dni robocze w godzinach 8:00 – 17:00
Czas podjęcia Konsultacji:	jeden dzień roboczy

11.2.13. Dostarczanie i wsparcie w instalacji Oprogramowania

W zakresie gwarancji Wykonawca zapewnia Zamawiającemu usługę dostarczania i wsparcia w instalacji oprogramowania dla uaktualnień oraz nowych wersji.

1) Dostarczanie oprogramowania:
   a) w okresie gwarancji Wykonawca będzie udostępniał Zamawiającemu aktualizacje całego dostarczonego oprogramowania, oprogramowania urządzeń do najnowszych wersji oferowanych przez producenta oprogramowania (włączając tzw. firmware). Dostęp do uaktualnienia musi być zapewniony bez dodatkowych opłat i ograniczeń ilościowych,
   b) aktualizacje będą dostarczane Zamawiającemu wraz ze szczegółową procedurą instalacji po przetestowaniu aktualizacji przez Wykonawcę i potwierdzeniu pozytywnego wyniku testów po stronie Wykonawcy,
   c) procedura instalacji będzie zawierała również szczegółowe informacje w zakresie wycofania zmian,
   d) w okresie gwarancji, Wykonawca zapewnia Zamawiającemu dostęp do usług wsparcia technicznego producenta urządzeń i oprogramowania właściwych dla danego Komponentu.
2) Wsparcie w instalacji aktualizacji/poprawek do oprogramowania:
   a) Wykonawca będzie świadczył Zamawiającemu wsparcie w ramach instalacji aktualizacji/poprawek do dostarczonego oprogramowania,
   b) Wykonawca może rekomendować, aby instalacja danego oprogramowania była zrealizowana przez Wykonawcę. W takim przypadku Wykonawca zgłasza taką rekomendację do Zamawiającego, podając uzasadnienie. Zamawiający po konsultacjach z Wykonawcą podejmuje decyzję, czy dane oprogramowanie zostanie zainstalowane przez Wykonawcę przy asyście Zamawiającego.
3) Poziom świadczenia usług

Wykonawca gwarantuje następujący poziom świadczenia usługi:
Dni robocze w godzinach 8:00 – 17:00

11.2.14. Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania i mobilnego urządzenia monitorującego.

W ramach usługi gwarancji, Wykonawca zobowiązany jest do:

1) dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego,
2) dołączenia do oferty oświadczenia producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta,
3) zapewnienia prawa do pobieranie uaktualnień oprogramowania układowego oraz sterowników, także po wygaśnięcia gwarancji na urządzenie,
4) zapewnienia możliwości sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji poprzez dedykowaną stronę producenta po podaniu numeru seryjnego urządzenia,
5) zapewnienia możliwości telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji poprzez ogólnopolską linię telefoniczną producenta po podaniu numeru seryjnego urządzenia,
6) zagwarantowana możliwości zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta,
7) zagwarantowana możliwości wymiany uszkodzonych dysków samodzielnie przez Zamawiającego bez utraty gwarancji,
8) dostarczenia wszystkich licencji wraz ze wsparciem, świadczonym przez Producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które musi umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Zamawiający wymaga, aby w przypadku wystąpienia problemów, wysyłanie zgłoszeń serwisowych do Producenta było zapewnione z poziomu portalu użytkownika, służącego do kompleksowego zarządzania kluczami licencyjnymi oprogramowania do wirtualizacji.
9) Wszystkie oferowane licencje powinny być bezterminowe i dostarczone na wszystkie węzły klastra wraz z 7-letnim wsparciem.
10) Producent rozwiązania musi udostępniać aktualizacje, do wszystkich opisanych Komponentów i muszą być one dostępne bezpłatnie podczas całego okresu wsparcia.

11.2.15. Szczegółowe wymagania gwarancji dotyczące stacji zarządzania oraz mobilnego urządzenia monitorującego

Wykonawca zobowiązuje się do udzielenia gwarancji zgodnie z poniższymi wymaganiami oraz w poniższych terminach

Przedmiot Zamówienia	Czas reakcji na zgłoszenie awarii (dni)	Czas naprawy/wymiany (dni)	Okres gwarancji (miesiące)
1	2	3	4
Stacja zarządzania Typ 1: – jednostka główna – monitor	1 dzień roboczy od zgłoszenia	Następny dzień roboczy od zgłoszenia jednostka główna,	60 miesięcy

–zestaw klawiatura mysz –stacja dokująca		2 dni robocze od zgłoszenia pozostałe elementy.	
Stacja zarządzania Typ 2: –jednostka główna –monitor –zestaw klawiatura mysz –stacja dokująca	1 dzień roboczy od zgłoszenia	Następny dzień roboczy od zgłoszenia jednostka główna, 10 dni roboczych od zgłoszenia monitor, 2 dni robocze od zgłoszenia pozostałe elementy.	60 miesięcy

Przez czas „naprawy/wymiany" rozumie się czas liczony od momentu zakończenia czasu reakcji na zgłoszenie do dokonania skutecznej naprawy albo wymiany wadliwego towaru na wolny od wad i dostarczenia sprzętu zastępczego.

Wymaganie dotyczące wszystkich typów Stacji Graficznych:

1) Gwarancja musi zapewniać ochronę komputera mobilnego przed uszkodzeniem fizycznym spowodowanymi typowymi zdarzeniami mogącymi powstać z winy użytkownika końcowego, takimi jak: upuszczenie, zalanie, skok napięcia (przepięcie) lub usterka zintegrowanego ekranu. W takim wypadku udzielający gwarancji zobowiązuje się do pokrycia pełnych kosztów naprawy, a w przypadku niemożności lub nieopłacalności naprawy – do dostarczenia nowej stacji. Wymagane jest, aby gwarancja obejmowała taką możliwość co najmniej trzy razy w okresie gwarancyjnym.
2) Gwarancja musi zapewniać w przypadku uszkodzenia dysku twardego oraz wymiany na nowy prawo do pozostawienia uszkodzonego dysku twardego u Zamawiającego w celu jego utylizacji przez Zamawiającego.
3) Gwarancja na baterię musi wynosić co najmniej 36 miesięcy.
4) Zamawiający wymaga zapewnienia możliwości sprawdzenia konfiguracji sprzętowej na dedykowanej do tego celu stronie producenta po podaniu numeru seryjnego urządzenia.
5) prawo do pobierania uaktualnień oprogramowania układowego oraz sterowników także po wygaśnięciu gwarancji na urządzenie,
6) Zamawiający wymaga aby warunki gwarancji były widoczne w systemie producenta na dedykowanej do tego celu stronie producenta po podaniu numeru seryjnego urządzenia zarówno w przypadku jednostki głównej jak również monitora oraz stacji dokującej,
7) w przypadku dłuższego czasu naprawy lub czasu wymiany aniżeli wskazany w kolumnie 3 w tabeli powyżej Wykonawca musi zapewnić Zamawiającemu w pełni sprawny asortyment o nie gorszych parametrach i funkcjonalności; dopuszcza się za zgodą Zamawiającego dostarczenie asortymentu zastępczego (oraz jego zwrotne odesłanie przez Zamawiającego) za pośrednictwem firmy kurierskiej na koszt i ryzyko Wykonawcy, a jego uruchomienie przez Wykonawcę nie jest wymagane; dostarczenie i uruchomienie takiego sprzętu zastępczego powoduje, że nie jest naliczana kara umowna za przekroczenie czasu naprawy/wymiany, pod warunkiem, że przekroczenie czasu

naprawy/wymiany będzie nie dłuższe niż 30 dni; po przekroczeniu tego terminu kara będzie naliczana.