

Spis treści

1. Definicje używane w dokumencie:.....	5
2. Serwery obliczeniowe.....	6
2.1. Serwer – parametry wspólne dla każdego typu serwera.....	6
2.2. Oprogramowanie do zarządzania serwerami z poziomu konsoli oprogramowania do zarządzania klastrem wirtualizacyjnym.....	11
2.3. Serwery obliczeniowe typu A, B, C.....	11
2.4. Serwer obliczeniowy typu „A”.....	12
2.5. Serwer obliczeniowy typu „B”.....	13
2.6. Serwer obliczeniowy typu „C”.....	13
2.7. Dodatkowe wyposażenie serwerów.....	14
2.7.1. Dysk SSD.....	14
2.7.2. Dysk HDD.....	14
2.7.3. Akcelerator graficzny typu „A”.....	14
2.7.4. Akcelerator graficzny typu „B”.....	15
2.7.5. Karta sieciowa 100GbE.....	16
2.7.6. Karta FPGAs.....	16
3. Serwer dyskowy.....	18
3.1. Serwer dyskowy typu „A”.....	18
3.2. Serwer dyskowy typu „B”.....	22
3.3. Serwer dyskowy typu „C”.....	26
4. Oprogramowanie do wirtualizacji.....	31
4.1. Wymagania wspólne dla wszystkich modułów oprogramowania do wirtualizacji.....	31
4.2. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji podstawowej.....	31
4.3. Oprogramowanie do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej w wersji rozszerzonej.....	34
4.4. Oprogramowanie do zarządzania klastrem wirtualizacyjnym.....	35
4.5. Oprogramowanie do wirtualizacji sieci.....	36
5. Infrastruktura sieciowa.....	38
5.1. Infrastruktura przełączająca i system sterujący.....	38
5.2. Moduły optyczne do interfejsów sieciowych.....	55
5.2.1. Moduł 1GbE, 1000BASE-T, SFP.....	55
5.2.2. Moduł 10GbE, BASE-T, SFP+.....	55
5.2.3. Moduł 10GbE, SR SFP+.....	56
5.2.4. Moduł 25 GbE, SR SFP28.....	56

Usunięte: 56

Usunięte: 56

Usunięte: 57

Usunięte: 57

Usunięte: 58

5.2.5.	Moduł 100GbE, LR4 QSFP28.....	<u>57</u>	Usunięte: 58
5.2.6.	Moduł 100GbE, SR4 QSFP28.....	<u>57</u>	Usunięte: 58
5.2.7.	Moduł 40 GbE, LR QSFP+.....	<u>57</u>	Usunięte: 59
5.2.8.	Moduł, 40 GbE, SR QSFP+.....	<u>58</u>	Usunięte: 59
5.3.	Okablowanie sieciowe.....	<u>58</u>	Usunięte: 59
5.3.1.	Patchcord UTP 3m.....	<u>58</u>	Usunięte: 59
5.3.2.	Patchcord UTP 5m.....	<u>58</u>	Usunięte: 60
5.3.3.	Patchcord UTP 10m.....	<u>58</u>	Usunięte: 60
5.3.4.	Patchcord LC-LC Multimode 3m.....	<u>58</u>	Usunięte: 60
5.3.5.	Patchcord LC-LC Multimode 5m.....	<u>59</u>	Usunięte: 60
5.3.6.	Patchcord LC-LC Single Mode 3m.....	<u>59</u>	Usunięte: 60
5.3.7.	Patchcord LC-LC Single Mode 5m.....	<u>59</u>	Usunięte: 60
5.3.8.	Patchcord MPO-MPO Multimode 3m – przełącznik -przełącznik.....	<u>59</u>	Usunięte: 60
5.3.9.	Patchcord MPO-MPO Multimode 5m – przełącznik -przełącznik.....	<u>59</u>	Usunięte: 61
5.3.10.	Kabel DAC pasywny 100G 3m.....	<u>59</u>	Usunięte: 61
5.3.11.	Kabel DAC pasywny 100G 5m.....	<u>60</u>	Usunięte: 61
5.3.12.	Kabel DAC pasywny breakout 100G --> 4 x 25 G 3m.....	<u>60</u>	Usunięte: 61
5.3.13.	Kabel DAC pasywny breakout 100G --> 4 x 25 G 5m.....	<u>60</u>	Usunięte: 61
5.3.14.	Kabel DAC pasywny 25G 3m.....	<u>60</u>	Usunięte: 61
5.3.15.	Kabel DAC pasywny 25G 5m.....	<u>60</u>	Usunięte: 61
6.	Stacje zarządzania.....	<u>61</u>	Usunięte: 62
6.1.	Stacja Zarządzania Typ 1.....	<u>61</u>	Usunięte: 62
6.1.1.	Jednostka główna spełniająca poniższe wymagania:.....	<u>61</u>	Usunięte: 62
6.1.2.	Monitor.....	<u>62</u>	Usunięte: 63
6.1.3.	Stacja dokująca.....	<u>62</u>	Usunięte: 63
6.1.4.	Zestaw klawiatura z myszą.....	<u>62</u>	Usunięte: 63
6.2.	Stacja Zarządzania Typ 2.....	<u>62</u>	Usunięte: 63
6.2.1.	Jednostka główna spełniająca poniższe wymagania:.....	<u>63</u>	Usunięte: 64
6.2.2.	Monitor.....	<u>64</u>	Usunięte: 65
6.2.3.	Stacja dokująca.....	<u>64</u>	Usunięte: 65
6.2.4.	Zestaw klawiatura z myszą.....	<u>64</u>	Usunięte: 65
6.3.	Stacja Zarządzania Typ 3.....	<u>64</u>	Usunięte: 65
6.3.1.	Jednostka główna spełniająca poniższe wymagania:.....	<u>64</u>	Usunięte: 65
6.3.2.	Monitor.....	<u>66</u>	Usunięte: 67
6.3.3.	Stacja dokująca.....	<u>66</u>	Usunięte: 67
6.3.4.	Zestaw klawiatura z myszą.....	<u>66</u>	Usunięte: 67

6.4. Monitor	66	Usunięte: 67
6.5. Stacja dokująca	66	Usunięte: 67
6.6. Zestaw klawiatura z myszą Typ A	67	Usunięte: 68
6.7. Zestaw klawiatura z myszą Typ B	67	Usunięte: 68
6.8. Opis równoważności	68	Usunięte: 69
7. Wdrożenie systemu	70	Usunięte: 71
7.1. Ramowy plan wdrożenia	70	Usunięte: 71
7.2. Dostawa i instalacja	72	Usunięte: 73
7.2.1. Ogólne wytyczne dotyczące dostawy i instalacji:	72	Usunięte: 73
7.2.2. Miejsce dostawy i instalacji poszczególnych Zadań	73	Usunięte: 74
7.2.3. Warunki instalacji dotyczące instalacji poszczególnych Zadań	74	Usunięte: 75
7.2.4. Szczegółowe wymagania dotyczące dostawy i instalacji dla poszczególnych Zadań, które musi spełnić Wykonawca	77	Usunięte: 78
7.3. Dokumentacja	79	Usunięte: 80
7.4. Dokumentacja Techniczna	79	Usunięte: 80
7.5. Dokumentacja Powykonawcza	80	Usunięte: 81
7.5.1. Wymagania	80	Usunięte: 81
7.6. Wytyczne do testów	82	Usunięte: 83
7.6.1. Testy weryfikacyjne	82	Usunięte: 83
7.6.2. Testy akceptacyjne (podstawowe i niezawodnościowe)	82	Usunięte: 83
7.6.3. Testy wydajnościowe	84	Usunięte: 85
7.6.4. Testy odbiorcze	85	Usunięte: 86
7.7. Odbiory	86	Usunięte: 87
8. Instrukcja	87	Usunięte: 88
8.1. Wstęp	87	Usunięte: 88
8.2. Zbiór wymagań dla instruktaży	87	Usunięte: 88
8.3. Zestawienie instruktaży wraz z czasem trwania	91	Usunięte: 92
9. Gwarancja	92	Usunięte: 93
9.1. Ogólne warunki Gwarancji	92	Usunięte: 93
9.2. Opis usługi Gwarancji	93	Usunięte: 94
9.2.1. Diagnostyka i rozwiązywanie problemów	93	Usunięte: 94
9.2.2. Klasyfikacja problemów	93	Usunięte: 94
9.2.3. Poziomy świadczenia usługi	94	Usunięte: 95
9.2.4. Wymiana informacji pomiędzy Zamawiającym a Wykonawcą	95	Usunięte: 96
9.2.5. Zgłaszanie problemów	96	
9.2.6. Czas reakcji	96	Usunięte: 97

9.2.7.	Rozwiązanie problemu	<u>96</u>	Usunięte: 97
9.2.8.	Czas rozwiązania problemu	97	
9.2.9.	Przywrócenie systemu.....	<u>97</u>	Usunięte: 98
9.2.10.	Czas przywrócenia systemu.....	<u>97</u>	Usunięte: 98
9.2.11.	Rozwiązanie zgłoszenia problemu.....	98	
9.2.12.	Konsultacje	<u>98</u>	Usunięte: 99
9.2.13.	Dostarczanie i wsparcie w instalacji Oprogramowania.....	99	
9.2.14.	Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania.....	<u>99</u>	Usunięte: 100
9.2.15.	Szczegółowe wymagania gwarancji dotyczące Stacji Zarządzania	<u>100</u>	Usunięte: 101

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 a;
- 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 obiektowa, 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 objętego danym Zadaniem.
- 8) **Zadanie** – pojedyncze zapotrzebowanie złożone przez Zamawiającego albo inny podmiot odbierający, realizowane niezależnie od innych zapotrzebowań.

2. Serwery obliczeniowe

2.1. Serwer – parametry wspólne dla każdego typu serwera

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ol style="list-style-type: none">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 umożliwi instalację dysków 2,5" SATA/SAS/NVMe.
Płyta główna	<ol style="list-style-type: none">1) Płyta główna z możliwością zainstalowania dwóch procesorów.2) Na płycie głównej muszą znajdować się co najmniej 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
Wbudowane porty	<ol style="list-style-type: none">1) Minimum 1 port Type-A w standardzie USB 2.0 lub wyższym na przednim panelu serwera.2) Minimum 1 port Type-A w standardzie USB 3.0 lub wyższym na tylnym panelu.3) Minimum 1 port VGA.
Wentylatory	<ol style="list-style-type: none">1) Redundantne typu Hot-Plug.
Bezpieczeństwo	<ol style="list-style-type: none">1) Panel przedni zamykany na klucz służący do ochrony przed nieautoryzowanym dostępem do dysków twardej.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 lub równoważny.6) Funkcjonalność włączania i wyłączania portów USB na obudowie.7) Możliwość wymazania danych z dysków znajdujących się wewnątrz serwera:<ol style="list-style-type: none">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.

	<p>9) Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego (ang. firmware) przed manipulacją ze strony złośliwego oprogramowania.</p> <ol style="list-style-type: none"> 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). <p>10) Serwer musi umożliwiać utworzenie bezpiecznego profilu w oparciu o konfigurację sprzętową oraz o konfigurację wewnętrznego oprogramowania komponentów serwera. Jakikolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi.</p> <p>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.</p>
Karta Zarządzania	<p>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:</p> <ol style="list-style-type: none"> 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 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 bezpośrednio poprzez złącze USB 16) monitorowanie zużycia dysków SSD 17) automatyczne zgłaszanie alertów do centrum serwisowego producenta

	<p>18) aktualizacje oprogramowania układowego (ang. firmware) dla wszystkich komponentów serwera</p> <p>19) przywrócenie poprzednich wersji oprogramowania układowego</p> <p>20) funkcję eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do/z pliku XML lub JSON</p> <p>21) funkcję automatycznego tworzenia kopii konfiguracji serwera w oparciu o zdefiniowany harmonogram</p> <p>22) wykrywanie odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji oprogramowania układowego serwera</p> <p>23) uruchomienie funkcjonalności umożliwiającej dostęp bezpośrednio poprzez urządzenia mobilne – funkcja konfiguracji oraz monitorowania najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/Apple iOS) używając jednego z protokołów BLE lub WIFI</p> <p>24) zdalne wyłączenia i włączenia portów USB</p> <p>25) mechanizm bezpiecznego wycofywania z eksploatacji poprzez automatyczne usuwanie poufnych danych w tym minimum:</p> <ol style="list-style-type: none"> a) konfiguracji BIOS b) konfiguracji kontrolera RAID c) dzienników systemowych d) danych konfiguracyjnych e) wszystkich danych z nośników wewnętrznych (dyski twarde, DCPMM, NVDIMM). <p>Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zamawiającego, 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).</p>
System do zarządzania	<p>1) System do zarządzania serwerami wraz z niezbędną licencją, który musi spełniać niżej wymienione wymagania:</p> <ol style="list-style-type: none"> a) integracja z 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, Linux 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

	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.
--	---

	<p>2) System może być zaoferowany jako prekonfigurowany obraz maszyny wirtualnej (ang. virtual appliance) dla zaoferowanego oprogramowania do wirtualizacji mocy obliczeniowej.</p> <p>3) Musi być dostępna dedykowana aplikacja na urządzenia mobilne (Android/Apple iOS) integrująca się z wyżej opisanym systemem do zarządzania.</p> <p>Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez zamawiającego, 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).</p>
Diagnostyka	<p>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)).</p>
Zasilacze	<p>1) Minimum 2 szt., redundancjne, typu Hot-Plug, o sprawności Platinum, o mocy zapewniającej poprawną pracę serwera w zaoferowanej konfiguracji przy pracy na połowie zainstalowanych zasilaczy.</p>
Certyfikaty	<p>1) Microsoft Windows Server min. w wersji 2022 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: https://www.windowsservercatalog.com/</p> <p>2) Red Hat Enterprise Linux (RHEL) min. w wersji 8 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: https://access.redhat.com/ecosystem/hardware</p> <p>3) VMware ESXi min. w wersji 7 – zgodność potwierdzona dla oferowanego modelu serwera na stronie: https://www.vmware.com/resources/compatibility/search.php</p>
Dokumentacja użytkownika	<p>1) Zamawiający wymaga dostarczenia dokumentacji w języku polskim lub angielskim w wersji elektronicznej.</p>

2.2. Oprogramowanie do zarządzania serwerami z poziomu konsoli oprogramowania do zarządzania klastrem wirtualizacyjnym

Oprogramowanie do zarządzania serwerami z poziomu konsoli oprogramowania do zarządzania klastrem wirtualizacyjnym (zwanej dalej konsolą wirtualizatora) musi być zintegrowane z zaferowaną konsolą oprogramowania do zarządzania klastrem wirtualizacyjnym (opisaną w niniejszych wymaganiach).

Wymagania, jakie musi spełniać to oprogramowanie:

- 1) możliwość instalowania poprawek podnoszących wersję oprogramowania układowego (ang. firmware) serwera wprost z konsoli wirtualizatora (wymagana zgodność z zaferowanym oprogramowaniem wirtualizacyjnym)
- 2) 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
- 3) 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
- 4) konsola wirtualizatora musi prezentować informacje wspierające serwisowanie takie jak:
 - a) numer serwisowy/seryjny serwera
 - b) data obowiązywania gwarancji
- 5) 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
- 6) 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

2.3. Serwery obliczeniowe typu A, B, C

Wymagania wspólne dla serwerów typu A, B, C

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	1) Wysokość 2 RU
Kontroler RAID	1) Sprzętowy kontroler dyskowy wspierający interfejs PCIe 4.0, z pojemnością cache minimum 4 GB, umożliwiającą 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 zaferowanym oprogramowaniem do wirtualizacji.

Interfejsy sieciowe	<ol style="list-style-type: none"> 1) Dwa interfejsy sieciowe o przepustowości minimum 1 Gb/s Ethernet w standardzie Base-T. 2) Dwuportowa karta sieciowa zainstalowana w serwerze jako karta rozszerzeń w slotcie PCIe 4.0, z gniazdami o przepustowości 100 Gb/s Ethernet w standardzie QSFP56, posiadająca: <ol style="list-style-type: none"> 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 dekapulacji 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 slotcie PCIe lub w slotcie 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: <ol style="list-style-type: none"> a) wsparcie dla wirtualizacji SR-IOV b) wsparcie dla enkapsulacji i dekapulacji dla protokołów VxLAN, NVGRE, Geneve c) wsparcie dla RoCE d) wsparcie dla Jumbo Frames o rozmiarach minimum 9 KB. <p>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.</p>
---------------------	--

2.4. Serwer obliczeniowy typu „A”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.3 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	<ol style="list-style-type: none"> 1) Zainstalowane 2 procesory 64-rdzeniowe, o taktowaniu co najmniej 2.0 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 605 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 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 do co najmniej 4 TB pamięci RAM.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski twarde hot-swap o pojemności minimum 480 GB każdy, SATA SSD do różnych zastosowań (ang. mixed-use) o współczynniku DWPD minimum 3 i rozmiarze 2,5", podłączone za pomocą zaoferowanego kontrolera RAID.

2.5. Serwer obliczeniowy typu „B”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.3 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
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. 393 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 4.0.
Pamięć RAM	1) Minimum 1 TB DDR4 RDIMM 3200 MT/s. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.
Dyski twarde	1) Zainstalowane 2 jednakowe dyski twarde hot-swap o pojemności minimum 480 GB każdy, SATA SSD do różnych zastosowań (ang. mixed-use) o współczynniku DWPD minimum 3 i rozmiarze 2,5", podłączone za pomocą zaoferowanego kontrolera RAID.

2.6. Serwer obliczeniowy typu „C”

Zaoferowany serwer musi spełniać wszystkie wymagania wspólne opisane w punkcie 2.1 oraz wymagania wspólne dla podzbioru typu serwów opisane w punkcie 2.3 oraz poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	1) Zainstalowane dwa procesory 16-rdzeniowe, o taktowaniu co najmniej 3.1 GHz, klasy x86-64 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku podstawowego (Base) min. 303 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 4.0.
Pamięć RAM	1) Minimum 512 GB DDR4 RDIMM 3200 MT/s. Płyta główna musi zapewniać obsługę co najmniej 4 TB pamięci RAM.

Dyski twarde	1) Zainstalowane 2 jednakowe dyski twarde hot-swap o pojemności minimum 480 GB każdy, SATA SSD do różnych zastosowań (ang. mixed-use) o współczynniku DWPD minimum 3 i rozmiarze 2,5", połączone za pomocą zaoferowanego kontrolera RAID.
--------------	---

2.7. Dodatkowe wyposażenie serwerów

Wszystkie poniższe elementy muszą być kompatybilne i możliwe do zainstalowania do zaoferowanych w ramach tego postępowania serwerach. Gwarancja na komponenty musi być na tych samych warunkach co na serwery.

2.7.1. Dysk SSD

Parametr	Charakterystyka (wymagania minimalne)
Typ	Dysk twardy w specyfikacji serwerowej, certyfikowany przez producenta serwera
Rodzaj nośnika	SSD
Interfejs	1 x SATA 6 Gb/s
Pojemność	480GB
Funkcje dodatkowe	1) Funkcja hot-swap 2) Dysk SSD zoptymalizowany pod kątem zapisu i odczytu danych (wykorzystanie mieszane)

2.7.2. Dysk HDD

Parametr	Charakterystyka (wymagania minimalne)
Typ	Dysk twardy w specyfikacji serwerowej, certyfikowany przez producenta serwera
Rodzaj nośnika	HDD
Prędkość obrotowa	10000 obr/min
Interfejs	SAS 12Gb/s
Pojemność	2,4 TB
Funkcje dodatkowe	1) Funkcja hot-swap

2.7.3. Akcelerator graficzny typu „A”

Parametr	Charakterystyka (wymagania minimalne)
Typ	Akcelerator graficzny w specyfikacji serwerowej, certyfikowany przez producenta serwera
Liczba graficznych rdzeni obliczeniowych	Min. 6192 rdzeni CUDA

Liczba rdzeni wspierających uczenie maszynowe	Min. 432 wyspecjalizowanych rdzeni wspierających uczenie maszynowe
Pamięć VRAM	Min. 80GB typu HBM2e o szerokości szyny danych 5120bit
Częstotliwość GPU	1) Bazowa: min. 1060MHz 2) Boost: min. 1400MHz
Częstotliwość pamięci	Min. 1510MHz
Wsparcie wirtualizacji	1) Wsparcie dla wirtualizacji karty graficznej, w szczególności wsparcie dla mechanizmów umożliwiających przekazanie karty graficznej do kontenerów uruchamianych z wykorzystaniem technologii Docker 2) Możliwość partycjonowania karty graficznej na co najmniej 7, niezależnych, zwirtualizowanych kart graficznych
Interfejs	1) Interfejs PCIe co najmniej w wersji 4.0 x16 ze wsparciem dla „Lane and polarity reversal” 2) Karty muszą być połączone ze sobą (każda z każdą) szyną dwukierunkową o przepustowości minimum 600GB/s
Wsparcie dla API obliczeniowych	Wymagane wsparcie dla min. 4 różnych API, np. CUDA, DirectCompute, OpenCL, OpenACC
Wydajność	Min. 19 TFLOPS dla obliczeń FP32 wg. deklaracji producenta
Zasilanie	Zużycie energii nie większe niż 300W, 8pinowe złącze zasilające

2.7.4. Akcelerator graficzny typu „B”

Parametr	Charakterystyka (wymagania minimalne)
Typ	Akcelerator graficzny w specyfikacji serwerowej, certyfikowany przez producenta serwera
Liczba graficznych rdzeni obliczeniowych	Min. 10752 rdzeni CUDA
Liczba rdzeni wspierających uczenie maszynowe	Min. 336 wyspecjalizowanych rdzeni wspierających uczenie maszynowe
Pamięć VRAM	Min. 48GB typu GDDR6 o szerokości szyny danych 384bit
Częstotliwość GPU	1) Bazowa: min. 1305MHz 2) Boost: min. 1740MHz
Częstotliwość pamięci	Min. 7250MHz
Wsparcie wirtualizacji	1) Wsparcie dla wirtualizacji karty graficznej, w szczególności wsparcie dla mechanizmów umożliwiających przekazanie karty graficznej do kontenerów uruchamianych z wykorzystaniem technologii Docker 2) Wsparcie dla technologii NVIDIA vPC/vApps, NVIDIA RTX Virtual Workstation, NVIDIA Virtual Compute Server

Interfejsy	1) Interfejs PCIe co najmniej w wersji 4.0 x16 ze wsparciem dla „Lane and polarity reversal” 2) 3 wyjścia DisplayPort 3) ▾
Multimedia	1) Min. 2 sprzętowe dekodery video 2) Min. 1 sprzętowy koder video
Wsparcie dla API obliczeniowych	Wymagane wsparcie dla min. 4 różnych API, CUDA, DirectCompute, OpenCL, OpenACC
Wydajność	Min. 37 TFLOPS dla obliczeń FP32 wg. deklaracji producenta
Zasilanie	Zużycie energii nie większe niż 300W, 8pinowe złącze zasilające

Usunięte: Karty muszą być połączone ze sobą (każda z każdą) szyną dwukierunkową o przepustowości minimum 600GB/s

2.7.5. Karta sieciowa 100GbE

Parametr	Charakterystyka (wymagania minimalne)
Typ	Karta sieciowa w specyfikacji serwerowej, certyfikowana przez producenta serwera
Maksymalna przepustowość	200Gb/s, 2 porty QSFP56
Interfejsy	1) Wsparcie dla prędkości 10/25/40/50/100/200GbE 2) Urządzenie przeznaczone do działania z interfejsem PCIe Gen4.0 x16,
Liczba portów	2 porty sieciowe
Wirtualizacja	Wsparcie dla SR-IOV oraz VirtIO
Cyberbezpieczeństwo	Sprzętowe wsparcie dla szyfrowania AES-GCM 128/256 dla protokołów IPSec i TLS. Wsparcie dla AES-XTS
Wydajność	DPDK message rate: min. 215Mpps
Wspierane funkcje	RoCE Programmable Congestion Control, IEEE 1588v2 (dokładność do poziomu nanosekund), Sprzętowe wsparcie enkapsulacji i dekapulacji dla VXLAN, NVGRE, Geneve

2.7.6. Karta FPGAs

Parametr	Charakterystyka (wymagania minimalne)
Typ	Akcelerator FPGA w specyfikacji serwerowej, certyfikowany przez producenta serwera
Pamięć	Min. 64GB pamięci DDR o min. przepustowości 75GB/s i wydajności min. 2400MT/s
Interfejsy	1) 2x QSFP28 100Gbps 2) PCI-e Gen3 x16
Liczba portów	2 porty sieciowe

Parametry FPGA	1) Min. 1182000 LUT 2) 2364000 rejestrów 3) 6840 DSP slices
Typ chłodzenia	Pasywne
Zasilanie	Maks. 250W

3. Serwer dyskowy

3.1. Serwer dyskowy typu „A”

Parametr	Charakterystyka (wymagania minimalne)
Zasoby dyskowe	<ol style="list-style-type: none">1) Serwer dyskowy / macierz dyskowa musi być dostarczona z minimum:<ol style="list-style-type: none">a) 18 jednakowymi dyskami SAS HDD 10k 2,5” – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 24 TiB. Pojemność użyteczną macierzy dyskowej 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.2) Zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 1 (jednego) dysku.3) W zaoferowanej konfiguracji dyskowej muszą być uwzględnione dyski zapasowe („Hot Spare”) w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 (jeden) zapasowy dysk na każdy serwer dyskowy.4) Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpocząć odtwarzanie danych na fizycznym dysku zapasowym.5) W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy).6) Kontrolery macierzy dyskowej muszą obsługiwać minimum 500 dysków.
Kontrolery macierzy dyskowej	<ol style="list-style-type: none">1) Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (ang. high availability cluster). Kontrolery muszą udostępniać dane poprzez protokoły iSCSI, Fibre Channel, CIFS oraz NFS.2) 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.3) W przypadku awarii zasilania dane niezapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.

	<p>4) Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze.</p> <p>5) Macierz musi mieć minimum 128 GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. Nie dopuszcza się stosowania pamięci na wymiennych dyskach jako podstawowego modułu cache.</p> <p>6) Macierz dyskowa musi realizować replikację (ang. mirroring) pamięci cache między kontrolerami.</p> <p>7) System operacyjny kontrolerów musi natywnie obsługiwać automatyczny „tiering” bloków danych pomiędzy dyskami SSD, SAS (macierz może alokować bloki dla danego wolumenu spośród wszystkich typów dysków: SSD, SAS równocześnie).</p> <p>8) Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie, minimum RAID 1 (lub 10), 5, 6.</p> <p>9) Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych.</p> <p>10) Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256 TB, plikowych o rozmiarze minimum 256 TB.</p> <p>11) Macierz musi posiadać wbudowaną funkcjonalność typu „thin provisioning” umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.</p>
Interfejsy	<p>1) Macierz musi być wyposażona w następujące, działające porty:</p> <ul style="list-style-type: none"> a) 4 porty 10 Gb/s Ethernet do podłączania serwerów, każdy port wyposażony w moduły optyczne SFP+ b) 2 porty 1 Gb/s Ethernet Base-T do zdalnego zarządzania kontrolerem c) 4 porty SAS minimum 12 Gb/s do podłączania półek dyskowych. <p>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.</p> <p>3) Porty przeznaczone do podłączenia serwerów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami).</p> <p>4) Musi być możliwość rozbudowy on-line macierzy do minimum 16 portów FC 32 Gb/s lub 25 Gb/s Ethernet jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów bądź usuwania zainstalowanych kart.</p>

Kopie migawkowe	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie „Copy On Write” dla dowolnego rodzaju danych (blokowe lub plikowe). 2) Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika. 3) System operacyjny macierzy dyskowej musi umożliwiać wykonywanie kopii migawkowych wolumenów plikowych w trybie „on-line” – bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen. 4) Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny. 5) Musi być możliwe udostępnienie kopii migawkowej w trybie do odczytu i zapisu. 6) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Microsoft SQL Server, Oracle Databases, VMware dla blokowych i plikowych „datastore” oraz zaofertowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składa swoje dane i wykonać kopie tylko tych wolumenów.
Obsługiwane protokoły	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i Fibre Channel – jeśli do uruchomienia potrzebna jest licencja, to Zamawiający wymaga jej dostarczenia. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, Fibre Channel oraz iSCSI są przedmiotem obecnego postępowania. 2) Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, itp. firm trzecich.
Pozostałe wymagania	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych. 2) System operacyjny macierzy, za pomocą interfejsu graficznego, musi mieć możliwość:

	<ul style="list-style-type: none"> a) konfiguracji macierzy dyskowej b) zbierania i wyświetlania informacji o stanie zasobów macierzy dyskowej c) prezentowania i gromadzenia zdarzeń zachodzących w macierzy dyskowej d) prezentowania bieżących statystyk wydajnościowych macierzy dyskowej e) podglądu parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym. <p>3) Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego.</p> <p>4) W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft (MS Active Directory).</p> <p>5) W celu zabezpieczania danych macierz dyskowa musi mieć mechanizm replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy. Macierz musi mieć mechanizm replikacji w trybie synchronicznym i asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gateway, serwer pośredniczący, etc. Musi istnieć funkcja odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być realizowana przy użyciu zewnętrznego oprogramowania. Licencja na replikację jest przedmiotem obecnego postępowania.</p> <p>6) System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (ang. Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub innych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu.</p> <p>7) Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy.</p> <p>8) Macierz musi posiadać funkcję zarządzania w sposób zautomatyzowany. Zamawiający dopuszcza możliwość zastosowania oprogramowania firm trzecich np. Ansible.</p> <p>9) Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez Zamawiającego to musi ona być dostarczona wraz z macierzą.</p> <p>10) Wszystkie kontrolery muszą posiadać tą samą liczbę portów w identycznej konfiguracji.</p>
Wymiana dysków	<ul style="list-style-type: none"> 1) Wymiana dysków może być dokonywana samodzielnie przez Zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski.

3.2. Serwer dyskowy typu „B”

Parametr	Charakterystyka (wymagania minimalne)
Zasoby dyskowe	<p>1) Serwer dyskowy / macierz dyskowa musi być dostarczona z minimum:</p> <p>a) 10 jednakowymi dyskami SSD 2,5" o współczynniku DWPD minimum 3 (w przypadku zastosowania dysków o DWPD mniejszym od 3 należy dostarczyć dwukrotnie większą pojemność na dyskach SSD) – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 10 TiB</p> <p>b) 9 jednakowymi dyskami SAS (HDD 10k lub SSD) 2,5" – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 12 TiB.</p> <p>Pojemność użyteczną macierzy dyskowej 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.</p> <p>2) Zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 1 (jednego) dowolnego dysku każdej grupy dysków wymienionych w punkcie 1) a) i 1) b).</p> <p>3) W zaoferowanej konfiguracji dyskowej muszą być uwzględnione dyski zapasowe („Hot Spare”) w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 (jeden) zapasowy dysk dla każdej grupy dysków wymienionych w punkcie 1) a) i 1) b). Dyski zapasowe nie mogą być wliczone do ilości dysków z punktu 1).</p> <p>4) Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpocząć odtwarzanie danych na fizycznym dysku zapasowym.</p> <p>5) W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy).</p> <p>6) Kontrolery macierzy dyskowej muszą obsługiwać minimum 500 dysków.</p>
Kontrolery macierzy dyskowej	<p>1) Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (ang. high availability cluster). Kontrolery muszą udostępniać dane poprzez protokoły iSCSI, Fibre Channel, CIFS oraz NFS.</p> <p>2) Obszar pamięci cache przeznaczony do zapisów danych musi posiadać lustrzaną kopię (ang. mirror).</p>

	<p>3) W przypadku awarii zasilania dane niezapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.</p> <p>4) Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze.</p> <p>5) Macierz musi mieć minimum 128 GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. Nie dopuszcza się stosowania pamięci na wymiennych dyskach jako podstawowego modułu cache.</p> <p>6) Macierz dyskowa musi realizować replikację (ang. mirroring) pamięci cache między kontrolerami.</p> <p>7) System operacyjny kontrolerów musi natywnie obsługiwać automatyczny „tiering” bloków danych pomiędzy dyskami SSD, SAS (macierz może alokować bloki dla danego wolumenu spośród wszystkich typów dysków: SSD, SAS równocześnie).</p> <p>8) Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie, minimum RAID 1 (lub 10), 5, 6.</p> <p>9) Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych.</p> <p>10) Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256 TB, plikowych o rozmiarze minimum 256 TB.</p> <p>11) Macierz musi posiadać wbudowaną funkcjonalność typu „thin provisioning” umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.</p>
Interfejsy	<p>1) Macierz musi być wyposażona w następujące, działające porty:</p> <ul style="list-style-type: none"> a) 8 portów 25 Gb/s Ethernet do podłączenia serwerów, każdy port wyposażony w moduł optyczny SFP28 b) 2 porty 1 Gb/s Ethernet Base-T do zdalnego zarządzania kontrolerem c) 4 porty SAS minimum 12 Gb/s do podłączenia półek dyskowych d) opcjonalnie 4 porty 10 Gb/s Ethernet do podłączenia serwerów, każdy port wyposażony w moduł optyczny SFP+. <p>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.</p> <p>3) Porty przeznaczone do podłączenia serwerów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami).</p> <p>4) Musi być możliwość rozbudowy on-line macierzy do minimum 16 portów FC 32 Gb/s lub 25 Gb/s Ethernet jedynie poprzez instalację dodatkowych kart</p>

	rozszerzeń bez konieczności instalacji dodatkowych kontrolerów bądź usuwania zainstalowanych kart.
Kopie migawkowe	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie „Copy On Write” dla dowolnego rodzaju danych (blokowe lub plikowe). 2) Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika. 3) System operacyjny macierzy dyskowej musi umożliwiać wykonywanie kopii migawkowych wolumenów plikowych w trybie „on-line” – bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen. 4) Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny. 5) Musi być możliwe udostępnienie kopii migawkowej w trybie do odczytu i zapisu. 6) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Microsoft SQL Server, Oracle Databases, VMware dla blokowych i plikowych „datastore” oraz zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składa swoje dane i wykonać kopie tylko tych wolumenów.
Obsługiwane protokoły	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i Fibre Channel – jeśli do uruchomienia potrzebna jest licencja to Zamawiający wymaga jej dostarczenia. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, Fibre Channel oraz iSCSI są przedmiotem obecnego postępowania. 2) Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, itp. firm trzecich.
Pozostałe wymagania	<ol style="list-style-type: none"> 1) System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych.

	<p>2) System operacyjny macierzy, za pomocą interfejsu graficznego, musi mieć możliwość:</p> <ul style="list-style-type: none"> a) konfiguracji macierzy dyskowej b) zbierania i wyświetlania informacji o stanie zasobów macierzy dyskowej c) prezentowania i gromadzenia zdarzeń zachodzących w macierzy dyskowej d) prezentowania bieżących statystyk wydajnościowych macierzy dyskowej e) podglądu parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym. <p>3) Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego.</p> <p>4) W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft (MS Active Directory).</p> <p>5) W celu zabezpieczenia danych macierz dyskowa musi mieć mechanizm replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy. Macierz musi mieć mechanizm replikacji w trybie synchronicznym i asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gateway, serwer pośredniczący, etc. Musi istnieć funkcja odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być realizowana przy użyciu zewnętrznego oprogramowania. Licencja na replikację jest przedmiotem obecnego postępowania.</p> <p>6) System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (ang. Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub innych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu.</p> <p>7) Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy.</p> <p>8) Macierz musi posiadać funkcję zarządzania w sposób zautomatyzowany. Zamawiający dopuszcza możliwość zastosowania oprogramowania firm trzecich np. Ansible.</p> <p>9) Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez Zamawiającego to musi ona być dostarczona wraz z macierzą.</p> <p>10) Wszystkie kontrolery muszą posiadać tę samą liczbę portów w identycznej konfiguracji.</p>
Wymiana dysków	<p>1) Wymiana dysków może być dokonywana samodzielnie przez Zamawiającego.</p> <p>2) Zamawiający zatrzymuje uszkodzone dyski.</p>

3.3. Serwer dyskowy typu „C”

Parametr	Charakterystyka (wymagania minimalne)
Zasoby dyskowe	<p>1) Serwer dyskowy / macierz dyskowa musi być dostarczona z minimum:</p> <p>a) 10 jednakowymi dyskami SSD 2,5" o współczynniku DWPD minimum 3 (w przypadku zastosowania dysków o DWPD mniejszym od 3 należy dostarczyć dwukrotnie większą pojemność na dyskach SSD) – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 22 TiB</p> <p>b) 9 jednakowymi dyskami SAS (HDD 10k lub SSD) 2,5" – pojemność użyteczna dla przestrzeni zbudowanej w oparciu o te dyski musi wynosić minimum 12 TiB.</p> <p>Pojemność użyteczną macierzy dyskowej 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.</p> <p>2) Zastosowane mechanizmy ochrony danych muszą zabezpieczać dane przed ich utratą w przypadku awarii co najmniej 1 (jednego) dowolnego dysku każdej grupy dysków wymienionych w punkcie 1) a) i 1) b).</p> <p>3) W zaoferowanej konfiguracji dyskowej muszą być uwzględnione dyski zapasowe („Hot Spare”) w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 (jeden) zapasowy dysk dla każdej grupy dysków wymienionych w punkcie 1) a) i 1) b). Dyski zapasowe nie mogą być wliczone do ilości dysków z punktu 1).</p> <p>4) Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpocząć odtwarzanie danych na fizycznym dysku zapasowym.</p> <p>5) W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy).</p> <p>6) Kontrolery macierzy dyskowej muszą obsługiwać minimum 500 dysków.</p>
Kontrolery macierzy dyskowej	<p>1) Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (ang. high availability cluster). Kontrolery muszą udostępniać dane poprzez protokoły iSCSI, Fibre Channel, CIFS oraz NFS.</p> <p>2) Obszar pamięci cache przeznaczony do zapisów danych musi posiadać lustrzaną kopię (ang. mirror).</p>

	<ol style="list-style-type: none"> 3) W przypadku awarii zasilania dane niezapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego w celu zachowania ich w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania. 4) Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze. 5) Macierz musi mieć minimum 128 GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. Nie dopuszcza się stosowania pamięci na wymiennych dyskach jako podstawowego modułu cache. 6) Macierz dyskowa musi realizować replikację (ang. mirroring) pamięci cache między kontrolerami. 7) System operacyjny kontrolerów musi natywnie obsługiwać automatyczny „tiering” bloków danych pomiędzy dyskami SSD, SAS (macierz może alokować bloki dla danego wolumenu spośród wszystkich typów dysków: SSD, SAS równocześnie). 8) Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie, minimum RAID 1 (lub 10), 5, 6. 9) Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych. 10) Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256 TB, plikowych o rozmiarze minimum 256 TB. 11) Macierz musi posiadać wbudowaną funkcjonalność typu „thin provisioning” umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.
Interfejsy	<ol style="list-style-type: none"> 1) Macierz musi być wyposażona w następujące, działające porty: <ol style="list-style-type: none"> a) 8 portów 25 Gb/s Ethernet do podłączenia serwerów, każdy port wyposażony w moduł optyczny SFP28 b) 2 porty 1 Gb/s Ethernet Base-T do zdalnego zarządzania kontrolerem c) 4 porty SAS minimum 12 Gb/s do podłączenia półek dyskowych d) opcjonalnie 4 porty 10 Gb/s Ethernet do podłączenia serwerów, każdy port wyposażony w moduł optyczny SFP+. 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) Porty przeznaczone do podłączenia serwerów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami).

	<p>4) Musi być możliwość rozbudowy on-line macierzy do minimum 16 portów FC 32 Gb/s lub 25 Gb/s Ethernet jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów bądź usuwania zainstalowanych kart.</p>
Kopie migawkowe	<p>1) System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie „Copy On Write” dla dowolnego rodzaju danych (blokowe lub plikowe).</p> <p>2) Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika.</p> <p>3) System operacyjny macierzy dyskowej musi umożliwiać wykonywanie kopii migawkowych wolumenów plikowych w trybie „on-line” – bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen.</p> <p>4) Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny.</p> <p>5) Musi być możliwe udostępnienie kopii migawkowej w trybie do odczytu i zapisu.</p> <p>6) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Microsoft SQL Server, Oracle Databases, VMware dla blokowych i plikowych „datastore” oraz zaoferowanego oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składa swoje dane i wykonać kopie tylko tych wolumenów.</p>
Obsługiwane protokoły	<p>1) System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i Fibre Channel – jeśli do uruchomienia potrzebna jest licencja, to Zamawiający wymaga jej dostarczenia. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, Fibre Channel oraz iSCSI są przedmiotem obecnego postępowania.</p> <p>2) Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, itp. firm trzecich.</p>
Pozostałe wymagania	<p>1) System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych.</p>

	<p>2) System operacyjny macierzy, za pomocą interfejsu graficznego, musi mieć możliwość:</p> <ul style="list-style-type: none"> a) konfiguracji macierzy dyskowej b) zbierania i wyświetlania informacji o stanie zasobów macierzy dyskowej c) prezentowania i gromadzenia zdarzeń zachodzących w macierzy dyskowej d) prezentowania bieżących statystyk wydajnościowych macierzy dyskowej e) podglądu parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym. <p>3) Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego.</p> <p>4) W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft (MS Active Directory).</p> <p>5) W celu zabezpieczenia danych macierz dyskowa musi mieć mechanizm replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy. Macierz musi mieć mechanizm replikacji w trybie synchronicznym i asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gateway, serwer pośredniczący, etc. Musi istnieć funkcja odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być realizowana przy użyciu zewnętrznego oprogramowania. Licencja na replikację jest przedmiotem obecnego postępowania.</p> <p>6) System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (ang. Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub innych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu.</p> <p>7) Wymagane jest szyfrowanie danych na dyskach. Należy dostarczyć niezbędne licencje na całą pojemność macierzy.</p> <p>8) Macierz musi posiadać funkcję zarządzania w sposób zautomatyzowany. Zamawiający dopuszcza możliwość zastosowania oprogramowania firm trzecich np. Ansible.</p> <p>9) Jeśli wymagana jest dodatkowa licencja na jakąkolwiek funkcjonalność wskazaną przez Zamawiającego to musi ona być dostarczona wraz z macierzą.</p> <p>10) Wszystkie kontrolery muszą posiadać tę samą liczbę portów w identycznej konfiguracji.</p>
Gwarancja	<p>1) 7 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania</p>

	awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Stałe monitorowanie macierzy przez zdalne centrum serwisowe.
Wymiana dysków	1) Wymiana dysków może być dokonywana samodzielnie przez Zamawiającego. 2) Zamawiający zatrzymuje uszkodzone dyski u siebie, bez konieczności ponoszenia dodatkowych opłat.

4. 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. Zaoferowanie oprogramowania do wirtualizacji pochodzącego wraz ze wszystkimi wymaganymi w danym zadaniu modułami od jednego producenta będzie dodatkowo punktowane.

4.1. 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.

4.2. 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 200MB 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 szeregowo, 3 porty równoległe i 20 urządzeń USB
 - h) wspierać następujące systemy operacyjne: Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 10, SLES 12, SLES 11, SLES 10, SLES 9, RHEL 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, Solaris 11, Solaris 10, Debian, CentOS, FreeBSD, Ubuntu, Mac OS X, Oracle Linux, CoreOS
 - 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 sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności co najmniej dla 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) umożliwiać aby konsola zarządzająca zaoferowanego oprogramowania posiadała możliwość przydzielania i konfiguracji uprawnień wraz z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP, dodatkowo umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS)~~
- q) zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- r) 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
- s) w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączenia do niego minimum dwóch fizycznych kart sieciowych
- t) posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN) na wirtualnych przełącznikach w zaoferowanym oprogramowaniu
- u) zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
- v) umożliwiać wykorzystanie technologii przepustowości sieci komputerowych 200 GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- w) obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- x) zapewniać możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- y) 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

- z) obsługiwać przełączenie ścieżek używanych przy dostępie do pamięci masowej bez utraty komunikacji w przypadku awarii jednej ze ścieżek
- aa) 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
- bb) 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)
- cc) w środowisku z minimum dwoma serwerami wirtualizacyjnymi musi zapewniać pracę bez przestoju 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
- dd) zapewniać możliwość obsługiwanie dysków wirtualnych maszyn do rozmiaru co najmniej 60 TB
- ee) posiadać funkcjonalność zarządzania poprzez ustandaryzowany interfejs programistyczny (API)
- ff) posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- gg) być kompatybilne z TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest 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
- hh) posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym 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
- ii) 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
- jj) wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol) i NTP (ang. Network Time Protocol)
- kk) posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych, w ramach klastra serwerów, w celu zwiększenia bezpieczeństwa dostępu warstwy wirtualizacji
- ll) 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
- mm) zapewniać podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa

- nn) 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
- oo) 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.

4.3. 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 4.2).
- 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 przestoju 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 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 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

4.4. 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 minimum: domenę Microsoft Active Directory i Open LDAP

- d) posiadać konsolę 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) być zgodne z oferowanym w ramach tego samego postępowania oprogramowaniem do wirtualizacji pamięci masowej i umożliwiać zarządzanie wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage)
- h) 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
- i) 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
- j) umożliwiać jednoczesną aktualizację oprogramowania na wielu dostarczanych wirtualizatorach
- k) 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
- l) 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
- m) 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 dostępuów administracyjnych do środowiska.

4.5. Oprogramowanie do wirtualizacji sieci

- 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), umożliwiającą 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 niezvirtualizowanym zdefiniowanego za pomocą technologii VLAN
- g) zapewniać funkcjonalność wirtualnego routera wspierającego protokół routingu BGP. Routing statyczny oraz BGP musi być możliwy do wykonania poprzez tunel GRE
- 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.

5. Infrastruktura sieciowa

5.1. Infrastruktura przełączająca i system sterujący

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

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
Typy i minimalne ilości wymaganych portów					
1	Ilość portów 400GbE (QSFP-DD)				
2	Ilość portów 100GbE (QSFP100)	32	8	4	
3	Ilość portów 1/10GbE (SFP+)				4
4	Ilość portów 1/10/25GbE (SFP+)		48		
5	Ilość portów 10GbE (10GBase-T)			48	
6	Ilość portów 1GbE (1000Base-T), wykluczając porty dedykowane do zarządzania				48
7	Interfejsy 400GbE muszą umożliwiać rozdzielanie na cztery interfejsy do pracy z szybkością 100GbE (ang. breakout)				
8	Interfejsy 100GbE muszą umożliwiać rozdzielanie na cztery interfejsy do pracy z szybkością 25GbE (ang. breakout)	Tak	Tak	Tak	
Parametry fizyczne i zasilanie					
1	Wysokość elementu liczona w jednostkach Rack Units [RU]	1RU	1RU	1RU	1RU
2	Przełącznik musi poprawnie pracować w temperaturze od 0 do 40 °C.	Tak	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	Tak
	W celu zachowania redundancji zasilania, każdy przełącznik	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>musi poprawnie działać po podłączeniu do dwóch niezależnych, obwodów napięcia przemiennego (AC). Znik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu przełącznika oraz ograniczenia jego funkcjonalności i 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.</p>				
5	<p>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 7.2.4, które należy uwzględnić przed realizacją zadania.</p>	Tak	Tak	Tak	Tak
6	<p>Przełącznik musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak np. karty z interfejsami sieciowymi, moduły optyczne) w trakcie pracy urządzenia (hot-swap).</p>	Tak	Tak	Tak	Tak
7	<p>Przełącznik musi umożliwiać instalację lub wymianę zasilaczy w trakcie pracy urządzenia (hot-swap).</p>	Tak	Tak	Tak	
Wymagania licencyjne i status urządzeń					
1	<p>Wszystkie przełączniki oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane z wyjątkiem</p>	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	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).				
2	Wszystkie Elementy przełączające wraz z działającym na nich oprogramowaniem sterującym muszą pochodzić od jednego producenta..	Tak	Tak	Tak	Tak
3	Elementy 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 (<u>dotyczy terytorium UE</u>), 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	Tak
4	Wszystkie interfejsy liniowe przełączników muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich	Tak	Tak	Tak	Nie

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>wykorzystanie dopiero po wprowadzeniu jakiegokolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych przełącznikach.</p>				
5	<p>Moduły optyczne (ang. transceiver) muszą pochodzić od producenta elementów sieciowych lub posiadać jego certyfikację do stosowania w elementach sieciowych. Jednakże karty liniowe, moduły lub porty przełącznika zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi, muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla 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.</p>	Tak	Tak	Tak	Tak
6	<p>Wszystkie Elementy przełączające 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</p>	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	wersji oprogramowania wyłącznie na potrzeby zamawiającego, nieoferowanej innym klientom.				
Minimalne wymagania wydajnościowe i pojemnościowe					
1	Wydajność przełączania co najmniej	6.4 Tbps	4.0 Tbps	1.7 Tbps	290Gbps
2	Liczba przetwarzanych pakietów na sekundę	2 Bpps	1 Bpps	1 Bpps	200Mpps
3	Czas przełączania ramek nie dłuższy niż	1 μs	1 μs	3 μs	3 μs
4	Całkowita wielkość buforów	32MB	32MB	12 MB	4MB
5	Minimalna liczba obsługiwanych adresów MAC	280 000	280 000	270 000	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	200 000	8 000
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	64 000	4 000
8	Obsługa protokołu MACSEC				
9	Ilość jednocześnie aktywnych VLANów	4000	4000	4000	1024
10	Całkowita maksymalna moc pobierana przez urządzenie	650 W	650 W	450 W	250 W
11	Maksymalna typowa moc pobierana przez urządzenie	400 W	400 W	350 W	250 W
Wymagania operacyjne					
1	Moduły optyczne dla interfejsów muszą umożliwiać sprawdzenie mocy odbieranego sygnału.	Tak	Tak	Tak	Tak
4	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	Tak	Nie

Usunięte: 2.5

Usunięte: 32

Usunięte: 280

Usunięte: 60

Usunięte: 370

Usunięte: 310

Usunięte: 350

Usunięte: 212

Usunięte: 200

Usunięte: 130

Usunięte: 220

Usunięte: 95

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
5	Elementy Przełączające muszą umożliwić konfigurację wykorzystując modele OpenConfig. Musi być zapewniona obsługa następujących protokołów: gRPC, RESTCONF, NETCONF.	Tak	Tak	Tak	Nie
6	Elementy Przełączające muszą zapewniać strumieniowanie danych telemetrycznych wykorzystując protokół NETCONF/gRPC lub w formacie GPB. Dane te muszą być poprawnie interpretowane i prezentowane w Systemie Zarządzania.	Tak	Tak	Tak	Nie
7	Wszystkie Elementy przełączające 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	Tak	Nie
8	Wszystkie Elementy przełączające muszą obsługiwać protokoły NTP i NTP6	Tak	Tak	Tak	Tak
9	Wszystkie Elementy przełączające muszą wspierać Precision Time Protocol (PTP, IEEE 1588v2)	Tak	Tak	Tak	Nie
10	Wszystkie Elementy przełączające muszą obsługiwać protokół LLDP	Tak	Tak	Tak	Tak
11	Wszystkie Elementy przełączające muszą umożliwiać dodanie wydzielonej tablicy routingu dla funkcji zarządzania (ang. Management VRF)	Tak	Tak	Tak	Nie
13	Wszystkie Elementy przełączające muszą zapewniać mechanizm sprzętowej ochrony przeciw atakowi przeciążającemu (ang. DoS) na	Tak	Tak	Tak	Nie

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	jednostkę sterującą CPU (ang. Control Plane Protection)				
Wymagania dla obsługi VXLAN					
1	Elementy przełączające muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie przy enkapsulacji musi być możliwa obsługa przełączania w warstwie L2 (ang. bridging).	Tak	Tak	Tak	Nie
2	Elementy przełączające muszą zapewniać sprzętową obsługę enkapsulacji VXLAN. Jednocześnie, przy enkapsulacji musi być możliwa obsługa routingu IP.	Tak	Tak	Tak	Nie
3	Elementy przełączające 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	Tak	Nie
4	Elementy przełączające 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 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	Tak	Tak	Tak	Nie

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2.5m				
Wymagania sieciowe					
1	Wszystkie Elementy przełączające 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	Tak
2	Wszystkie Elementy przełączające muszą obsługiwać funkcję IGMP snooping (dla IGMPv2 oraz IGMPv3).	Tak	Tak	Tak	Tak
3	Wszystkie Elementy przełączające muszą obsługiwać agregację interfejsów z wykorzystaniem protokołu LACP (IEEE 802.3ad)	Tak	Tak	Tak	Tak
4	Wszystkie Elementy przełączające muszą umożliwiać stworzenie protekcji terminującej zagregowane interfejsy (LAG) na dwóch 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 połączenia zagregowanego. Jeśli implementacja protekcji wymaga dodatkowych portów które przenoszą ruch w czasie awarii wykonawca musi dostarczyć odpowiednie okablowanie o długości minimum 2,5m	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
5	Wszystkie Elementy przełączające muszą obsługiwać 802.1w RSTP, 802.1s MSTP.	Tak	Tak	Tak	Tak
6	Wszystkie Elementy przełączające muszą umożliwiać tworzenie list bezpieczeństwa (ang. ACLs) na warstwie L2 (MAC ACL), warstwie L3 (IP) i warstwie L4 (porty).	Tak	Tak	Tak	Tak
7	Wszystkie Elementy przełączające muszą obsługiwać protokół 802.1Qbb PFC (Priority-based Flow Control).	Tak	Tak	Tak	Nie
8	Wszystkie Elementy przełączające muszą umożliwiać regulację (ang. Shaping) wielkości ruchu wyjściowego.	Tak	Tak	Tak	Nie
10	Wszystkie Elementy przełączające zapewniać statyczny routing IP oraz dynamiczny routing IP zgodny z OSPFv2, OSPFv3, BGP, RIPv2.	Tak	Tak	Tak	Tak
11	Wszystkie Elementy przełączające muszą zapewniać mechanizm dystrybucji pakietów IP poprzez ścieżki z równym kosztem (ang. Equal Cost Multi-Path routing ECMP).	Tak	Tak	Tak	Tak
12	Wszystkie Elementy przełączające muszą zapewniać możliwość tworzenia polityk dla routing IP (ang. Route Maps).	Tak	Tak	Tak	Nie
13	Wszystkie Elementy przełączające muszą zapewniać możliwość dystrybucji informacji routingowych pomiędzy różnymi wirtualnymi tablicami routingowymi (ang. VRF route leaking).	Tak	Tak	Tak	Nie
14	Wszystkie Elementy przełączające muszą obsługiwać protokół BFD.	Tak	Tak	Tak	Nie

System Zarządzania

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
Wymagania ogólne					
1	Licencja dostarczona wraz z systemem zarządzania nie może ograniczać liczby ani użytkowników, ani administratorów korzystających jednocześnie z platformy systemu zarządzania.	Tak	Tak	Tak	Tak
2	System Zarządzania musi być dostarczony jako skonfigurowany obraz maszyny wirtualnej do uruchomienia na platformie KVM lub VMWare. Maksymalne wymagania Systemu Zarządzania nie mogą przekroczyć 16 cores CPU, 32 GB RAM, 1TB HDD. Jeśli System Zarządzania przekracza te wymagania wykonawca musi dostarczyć platformę sprzętową, która zapewni odpowiednie parametry.	Tak	Tak	Tak	Tak
3	Licencja dostarczona wraz z systemem zarządzania musi umożliwić stworzenie klastra maszyn wirtualnych pracujących w trybie wysokiej dostępności tak, aby awaria wyłączająca jedną z maszyn wirtualnych nie powodowała przerwy w działaniu systemu zarządzania.	Tak	Tak	Tak	Tak
4	Interfejs użytkownika systemu zarządzania musi być dostępny z poziomu przeglądarki WWW z prawidłowym obsługą co najmniej następujących przeglądarek: Microsoft Edge, Google Chrome, Firefox	Tak	Tak	Tak	Tak
5	System zarządzania musi obsługiwać jednoczesną pracę wielu użytkowników.	Tak	Tak	Tak	Tak
7	System Zarządzania musi zapewniać możliwość zdalnego aktualizowania Elementów przełączających, z możliwością wycofania i przywrócenia poprzedniej wersji.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
8	System Zarządzania musi zapewniać możliwość zapisania i odtworzenia kopii zapasowej Modułów Konfiguracyjnych.	Tak	Tak	Tak	Tak
9	System Zarządzania musi zapewniać możliwość wykorzystania interfejsu programistycznego (REST API) do wykonywania typowych operacji konfigurowania takich jak tworzenie, dodawanie i implementowanie Modułów Konfiguracyjnych	Tak	Tak	Tak	Tak
10	Niedostępność systemu zarządzania nie może mieć jakiegokolwiek wpływu na urządzenia sieciowe zintegrowane z systemem zarządzania. W szczególności nie może uniemożliwiać lub ograniczać możliwości konfigurowania urządzeń sieciowych za pomocą interfejsu CLI.	Tak	Tak	Tak	Tak
11	System zarządzania musi posiadać możliwość realizacji funkcji AAA poprzez integrację z zewnętrznym serwerem Radius oraz z zewnętrznym serwerem TACACS (przy czym nie jest wymagana integracja z dwoma tymi serwerami jednocześnie)	Tak	Tak	Tak	Tak
12	System zarządzania musi posiadać możliwość integracji z zewnętrznymi dostawcami usług uwierzytelnienia i tożsamości z wykorzystaniem standardów OAuth i SAML.	Tak	Tak	Tak	Tak
13	System musi umożliwiać tworzenie token-ów dostępowych wykorzystywanych jako mechanizm uwierzytelnienia do REST API, które eksponuje system zarządzania. System musi umożliwiać przypisywanie uprawnień do poszczególnych	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	token-ów w oparciu o role dostępowe. Te same role dostępowe powinny być wykorzystywane do zarządzania uprawnieniami użytkowników GUI.				
Wymagania dla funkcji monitorowania					
1	System Zarządzania musi zbierać i prezentować alarmy generowane przez Elementy Przełączające. Alarmy muszą obejmować zdarzenia generowane przez syslog, zmiany stanu interfejsów, przekroczenia progów błędów na interfejsach wejściowych (CRC), przeciążenia ruchowe interfejsów wejściowych i wyjściowych. System Zarządzania musi zapewnić mechanizm potwierdzania alarmów i dodawania komentarzy. System Zarządzania musi zapewnić mechanizm wyróżniania ważności alarmów i zdarzeń oraz możliwość ich modyfikacji. Przy wyświetlaniu alarmów powinna być możliwość filtrowania alarmów pod kątem ważności.	Tak	Tak	Tak	Tak
2	System zarządzania musi umożliwiać zbieranie i wizualizacja następujących parametrów: Parametry urządzenia: wykorzystanie CPU, pamięci RAM, temperatura pracy. Interfejsy: stan pracy (aktywny, wyłączony, itp.), statystyki ruchowe dla transmisji i odbioru, statystyki błędów, wartość MTU Ethernet: tablica MAC, wpisy ARP IP routing: zbudowana tablica routingu IPv4 i IPv6, (wliczając wirtualne tablice routingu VRF),	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	BGP: numery AS, zestawione sąsiedztwa Parametry muszą być wizualizowane w czasie rzeczywistym oraz historycznie z możliwością wyboru dowolnego przedziału czasowego z ostatniego miesiąca zbieranych danych. System Zarządzania musi umożliwiać budowanie i komponowanie własnych zestawień parametrów do obserwacji.				
3	System zarządzania musi zapewniać wizualizację topologii połączeń. Topologia połączeń musi być automatycznie wykrywana i budowana.	Tak	Tak	Tak	Tak
4	Na planie topologii system zarządzania musi wizualizować: wydarzenia i alarmy, szybkości interfejsów, wykorzystanie pasma, błędy w postaci utraconych pakietów, przepływy pakietów dla wskazanych par IP i protokołów.	Tak	Tak	Tak	Tak
5	System zarządzania musi zbierać i prezentować parametry jakości transmisji pomiędzy Elementami przełączającymi. Parametry określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss).	Tak	Tak	Tak	Tak
6	System zarządzania musi zbierać i prezentować informację o przepływach pakietów danych w postaci par IP i protokołów, dopuszcza się prezentacje poprzez raport sflow.	Tak	Tak	Tak	Tak
7	System zarządzania musi umożliwiać wyszukiwanie adresów IP oraz MAC widocznych z poziomu	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	Elementów przełączających. Możliwość wyszukiwania dotyczy adresów statycznych i dynamicznych tablicach poszczególnych Elementów. Odnalezione adresy muszą być prezentowane wraz z kontekstem opisującym Elementy oraz interfejsy/tablice związane z danym adresem.				
8	System zarządzania musi umożliwiać porównywanie i wizualizację różnic pomiędzy parametrami dla dwu dowolnych Elementów przełączających we wskazanych momentach czasowych. Parametrami podlegającymi porównaniu muszą być konfiguracje urządzeń.	Tak	Tak	Tak	Tak
9	System Zarządzania musi na bieżąco (bez wymuszenia) sygnalizować modyfikację konfiguracji wykonaną z poziomu konsoli Elementów przełączających, która wprowadza różnicę pomiędzy konfiguracją budowaną przez System Zarządzania a wprowadzoną na urządzeniu. Administrator Systemu Zarządzania powinien mieć możliwość przywrócenia poprzedniej konfiguracji lub akceptacji zmian dokonanych na poziomie konsoli.	Tak	Tak	Tak	Tak
Wymagania dla funkcji zestawiania usług (ang. provisioning)					
1	System Zarządzania musi zapewnić automatyczną procedurę budowania konfiguracji początkowej (ang. ZTP „Zero Touch Provisioning”). W szczególności, nowe urządzenie, z konfiguracją fabryczną, po podłączeniu do sieci, powinno za pomocą DHCP odnaleźć system zarządzania a następnie pobrać	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	konfigurację początkową i automatycznie zintegrować się z systemem zarządzania. Proces ten musi uwzględniać automatyczną aktualizację oprogramowania urządzenia sieciowego do wskazanej wersji.				
2	System Zarządzania musi zapewnić automatyczną procedurę ładowania konfiguracji przy wymianie urządzenia (ang. „Zero Touch Replacement”). W szczególności, nowe urządzenie, z konfiguracją fabryczną, po podłączeniu do sieci, powinno za pomocą DHCP odnaleźć system zarządzania a następnie pobrać konfigurację urządzenia zastępowanego. Proces ten musi uwzględniać automatyczną aktualizację oprogramowania urządzenia sieciowego do takiej samej wersji jaka była wykorzystywana na urządzeniu zastępowanym.	Tak	Tak	Tak	Tak
3	System Zarządzania musi umożliwiać budowanie konfiguracji Elementów. Konfiguracja musi być zgodna z konfiguracją tworzoną z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface / CLI). Za pomocą systemu zarządzania musi istnieć możliwość skonfigurowania wszystkich parametrów Elementów przełączających.	Tak	Tak	Tak	Tak
4	Zintegrowanie Elementów przełączających z systemem zarządzania nie może wykluczać bezpośredniej pracy z interfejsami administracyjnymi Elementów.	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	Rozwiązanie musi umożliwiać wymienną konfigurację Elementów: poprzez System Zarządzania lub bezpośrednio z wykorzystaniem interfejsu tekstowego (ang. CLI).				
5	System Zarządzania musi umożliwiać definiowanie sekcji konfiguracji urządzeń, które są zarządzane poza Systemem Zarządzania i które mają przez System Zarządzania być ignorowane.	Tak	Tak	Tak	Tak
6	System Zarządzania musi wykrywać i wizualizować rozbieżności pomiędzy konfiguracją wynikającą z parametrów zdefiniowanych na Systemie Zarządzania oraz parametrów skonfigurowanych bezpośrednio na urządzeniach sieciowych.	Tak	Tak	Tak	Tak
7	System Zarządzania musi dostarczyć mechanizm budowania konfiguracji Elementów z wykorzystywaniem Modułów Konfiguracyjnych (części konfiguracji CLI). Musi istnieć możliwość wykorzystania Modułów Konfiguracyjnych w trybie hierarchicznym, to znaczy że Moduł Konfiguracji jest dziedziczony przez wszystkie Elementy znajdujące się w danej hierarchii. Modyfikacja Modułu Konfiguracji musi powodować odpowiednią zmianę konfiguracji wszystkich Elementów znajdujących się w danej hierarchii.	Tak	Tak	Tak	Tak
8	Moduły Konfiguracji muszą być dostępne w trybie tekstowym (analogicznie jak pliki konfiguracyjne interfejsu tekstowego CLI). Ponadto, musi istnieć mechanizm	Tak	Tak	Tak	Tak

l.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	<p>automatyzacji tworzenia Modułów Konfiguracyjnych wykorzystując języka skryptów oparty na języku Python lub Perl. Tworzenie, testowanie, uruchamianie i zarządzanie skryptami Python/Perl musi w całości odbywać się poprzez interfejs GUI systemu zarządzania i musi stanowić integralną część tego systemu.</p>				
9	<p>System Zarządzania musi dostarczyć mechanizm weryfikacji oczekiwanych wyników przed implementacją Modułów Konfiguracyjnych na Elementach Przełączających. Po implementacji zmian konfiguracyjnych opisanych w Modułach Konfiguracyjnych musi istnieć mechanizm wycofania tych zmian.</p>	Tak	Tak	Tak	Tak
10	<p>System Zarządzania musi umożliwiać proces automatyzacji wielu zmian konfiguracyjnych i grupowania ich w pakiety. W ramach pakietów zmian, musi istnieć możliwość konfigurowania kolejności wykonywania poszczególnych zmian. System Zarządzania musi umożliwiać wybranie wykonywania zmian w pakiecie sekwencyjnie lub równolegle. System musi umożliwiać wykonywanie niestandardowych akcji (np. wykonania skryptu) jako jeden z elementów pakietów zmian. System musi umożliwiać zatrzymanie wykonywania kolejnych zmian w sekwencji, jeżeli zamiany je poprzedzające się nie powiedą.</p>	Tak	Tak	Tak	Tak
11	<p>System zarządzania musi umożliwiać tworzenie własnej biblioteki pomocniczych skryptów, napisanych w języku</p>	Tak	Tak	Tak	Tak

I.p	Wymaganie	100GbE	25GbE	10GbE	1GbE
	Python lub Perl, które mogą być uruchamiane i parametryzowane z poziomu Systemu Zarządzania. Tworzenie, testowanie, uruchamianie i zarządzanie skryptami Python/Perl musi w całości odbywać się poprzez interfejs GUI systemu zarządzania i musi stanowić integralną część tego systemu.				

5.2. Moduły optyczne do interfejsów sieciowych

5.2.1. Moduł 1GbE, 1000BASE-T, SFP

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł 1000BASE-T SFP
Kompatybilność	Moduł musi być zgodny ze standardem SFP Multi Source Agreement (MSA) – Small Form Factor Pluggable (SFP) Transceiver Multi-Source Agreement (MSA), September 2000
Interfejs	<ol style="list-style-type: none"> 1) Moduł musi posiadać interfejs Gigabit Ethernet (1000BASE-T) zgodnie ze standardem IEEE Std 802.3 2) Wymaga się funkcji negocjacji szybkości łącza (10Mbit/s, 100Mbit/s, 1Gbit/s) i trybu pracy (full duplex, half duplex). 3) Moduł musi być wyposażony w złącze RJ-45
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 10/100/1000 Mb/s
Dodatkowe	<ol style="list-style-type: none"> 1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się, by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.2. Moduł 10GbE, BASE-T, SFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł BASE-T SFP+
Kompatybilność	<p>Moduł musi być zgodny ze standardami:</p> <ol style="list-style-type: none"> 1) SFF-8431 – “Specifications for Enhanced 8.5 and 10 Gigabit Small Form Factor Pluggable Module ‘SFP+ ’”, SFF Document Number SFF-8431, Revision 3.0.

Interfejs	1) Moduł musi posiadać interfejs 10GBASE-T zgodnie ze standardem IEEE 802.3an. 2) Moduł musi być wyposażony w złącze RJ-45
Zasięg	min. 30m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 10 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.3. Moduł 10GbE, SR SFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR SFP+
Kompatybilność	Moduł musi być zgodny ze standardami: 1) SFF-8431 – “Specifications for Enhanced 8.5 and 10 Gigabit Small Form Factor Pluggable Module ‘SFP+ ’”, SFF Document Number SFF-8431, Revision 3.0.
Interfejs	Moduł musi posiadać interfejs 10GBASE-SR zgodnie ze standardem IEEE 802.3ae. Moduł musi być wyposażony w złącze LC Duplex
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 10 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.4. Moduł 25 GbE, SR SFP28

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR SFP28
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3by dla interfejsu 25GBase-SR4
Interfejs	Moduł musi być wyposażony w interfejs LC Duplex
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 25 Gb/s oraz 10 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania.

	2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).
--	---

5.2.5. Moduł 100GbE, LR4 QSFP28

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł LR4 QSFP28
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3ba dla interfejsu 100GBase-LR4
Interfejs	Moduł musi być wyposażony w złącze LC Duplex
Zasięg	min. 10km
Przepustowość	Moduł musi umożliwiać pracę z prędkością 100 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.6. Moduł 100GbE, SR4 QSFP28

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR4 QSFP28
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3bm dla interfejsu 100GBase-SR4
Interfejs	Moduł musi być wyposażony w złącze MTP/MPO-12
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 100 Gb/s
Dodatkowe	1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.2.7. Moduł 40 GbE, LR QSFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł LR QSFP+
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3ba dla interfejsu 40GBase-LR4
Interfejs	Moduł musi być wyposażony w złącze LC Duplex
Zasięg	min. 10km
Przepustowość	Moduł musi umożliwiać pracę z prędkością 40 Gb/s

Dodatkowe	<ol style="list-style-type: none"> 1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).
-----------	--

5.2.8. Moduł, 40 GbE, SR QSFP+

Parametr	Charakterystyka (wymagania minimalne)
Typ	Moduł SR QSFP+
Kompatybilność	Moduł musi być zgodny ze standardem IEEE 802.3ba dla interfejsu 40GBase-SR4
Interfejs	Moduł musi być wyposażony w złącze MTP/MPO-12
Zasięg	min. 100m
Przepustowość	Moduł musi umożliwiać pracę z prędkością 40 Gb/s
Dodatkowe	<ol style="list-style-type: none"> 1) Moduł musi być kompatybilny z urządzeniami sieciowymi (przełączniki), interfejsami sieciowymi w serwerach i serwerach dyskowych (macierzach dyskowych) dostarczanych w ramach tego postępowania. 2) Wymaga się by moduł mógł być instalowany w urządzeniu i wyjmowany z urządzenia podczas jego pracy (Hot-Pluggable).

5.3. Okablowanie sieciowe

Zaferowane okablowanie musi być kompatybilne i działać prawidłowo z zaferowanymi kartami sieciowymi w serwerach, serwerach dyskowych oraz przełącznikami sieciowymi.

5.3.1. Patchcord UTP 3m

Typ i parametry	UTP kat. 6
Długość	3m
Złącza	RJ45

5.3.2. Patchcord UTP 5m

Typ i parametry	UTP kat. 6
Długość	5m
Złącza	RJ45

5.3.3. Patchcord UTP 10m

Typ i parametry	UTP kat. 6
Długość	10m
Złącza	RJ45

5.3.4. Patchcord LC-LC Multimode 3m

Typ i parametry p	LC UPC to LC UPC Duplex OM5 Multimode
-------------------	---------------------------------------

Długość	3m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	LC/UPC

5.3.5. Patchcord LC-LC Multimode 5m

Typ i parametry	LC UPC to LC UPC Duplex OM5 Multimode
Długość	5m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	LC/UPC

5.3.6. Patchcord LC-LC Single Mode 3m

Typ i parametry	LC UPC to LC UPC Duplex OS2 Single Mode
Długość	3m
Tłumienność	tłumienność złącza nie większa niż 0,25 dB
Złącza	LC/UPC

5.3.7. Patchcord LC-LC Single Mode 5m

Typ i parametry	LC UPC to LC UPC Duplex OS2 Single Mode
Długość	5m
Tłumienność	tłumienność złącza nie większa niż 0,25 dB
Złącza	LC/UPC

5.3.8. Patchcord MPO-MPO Multimode 3m – przełącznik -przełącznik

Typ i parametry	MPO to MPO OM4 Multimode – 12 włókien
Długość	3m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	MPO/MTP
Kompatybilność	Patchcord musi gwarantować poprawną łączność pomiędzy dwoma dostarczonymi przełącznikami sieciowymi dla portów 100Gb/s

5.3.9. Patchcord MPO-MPO Multimode 5m – przełącznik -przełącznik

Typ i parametry	MPO to MPO OM4 Multimode – 12 włókien
Długość	5m
Tłumienność	tłumienność złącza nie większa niż 0,35 dB
Złącza	MPO/MTP
Kompatybilność	Patchcord musi gwarantować poprawną łączność pomiędzy dwoma dostarczonymi przełącznikami sieciowymi dla portów 100Gb/s

5.3.10. Kabel DAC pasywny 100G 3m

Typ i parametry	DAC pasywny 100G QSFP28
Długość	3m
Złącza	QSFP28

5.3.11. Kabel DAC pasywny 100G 5m

Typ i parametry	DAC pasywny 100G QSFP28
Długość	5m
Złącza	QSFP28

5.3.12. Kabel DAC pasywny breakout 100G --> 4 x 25 G 3m

Typ i parametry	DAC pasywny 100G QSFP28 to 4 x 25G SFP28 Breakout
Długość	3m
Złącza	QSFP28 – 4 x SFP28

Usunięte: 5m

5.3.13. Kabel DAC pasywny breakout 100G --> 4 x 25 G 5m

Typ i parametry	DAC pasywny 100G QSFP28 to 4 x 25G SFP28 Breakout
Długość	5m
Złącza	QSFP28 – 4 x SFP28

5.3.14. Kabel DAC pasywny 25G 3m

Typ i parametry	DAC pasywny 25G SFP28
Długość	3m
Złącza	SFP28

5.3.15. Kabel DAC pasywny 25G 5m

Typ i parametry	DAC pasywny 25G SFP28
Długość	5m
Złącza	SFP28

6. Stacje zarządzania

6.1. Stacja Zarządzania Typ 1

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

6.1.1. Jednostka główna spełniająca poniższe wymagania:

- 1) Wyświetlacz: 15,6" cala, rozdzielczość 3840x2400, jasność min. 500 nit, z powłoką przeciwoodblaskową;
- 2) Procesor: zgodny z x64, posiadający co najmniej 14 fizycznych rdzeni, w dwóch klasach wydajności (co najmniej 6 rdzeni zapewniających wydajność i co najmniej 8 rdzeni energooszczędnych), co najmniej 20 wątków. Zaprojektowany do pracy w mobilnych stacjach roboczych (pobór mocy w podstawowym trybie pracy nie więcej niż 45W, w trybie turbo nie więcej niż 115W), co najmniej 24MB cache, osiągający wydajność minimum: 28700 punktów Passmark CPU Mark w teście wydajności Pass Mark Performance Test (stan na 25.10.2022), pracujący z minimalną częstotliwością w trybie turbo dla rdzeni energooszczędnych 3,80GHz oraz dla rdzeni zapewniających wydajność 5GHz ;
- 3) Pamięć RAM: nie mniej niż 64 GB, min. DDR4;
- 4) Dysk twarde: nie mniej niż jeden dysk o pojemności 2TB w technologii M.2 SSD PCIe Gen4 x4 NVMe, musi być możliwość instalacji drugiego dysku. Po instalacji drugiego dysku musi być możliwe skonfigurowanie obu dysków w trybie RAID 0 lub 1;
- 5) Dodatkowa karta graficzna z min. 4GB RAM;
- 6) Zintegrowane porty (co najmniej):
 - a) min. 2x gniazdo Thunderbolt 4 Type-C,
 - b) zintegrowany czytnik kart SD/SDHC/SDXC,
 - c) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm,
 - d) min. jedno gniazdo HDMI wbudowane lub realizowane poprzez Thunderbolt Type-C (w takim przypadku wymagane jest dostarczenie przejściówki z USB-C do HDMI – gniazdo),
 - e) min. 1x gniazdo USB Type-A wbudowany lub realizowany poprzez Thunderbolt Type-C (w takim przypadku wymagane jest dostarczenie przejściówki z USB Type-C do USB Type-A – gniazdo),Uwaga: Zamawiający dopuszcza, aby gniazdo HDMI oraz USB Type-A były realizowane poprzez port Thunderbolt Type-C za pomocą jednej przejściówki (w takim przypadku wymagane jest dostarczenie przejściówki z USB Type-C do HDMI – gniazdo / USB Type-A gniazdo).
- 7) Komunikacja:
 - a) Wi-Fi 6 dwuzakresowa zgodna z co najmniej IEEE 802.11 ax/ac/a/b/g/n,
 - b) 1x LAN 10/100/1000 Ethernet wbudowana lub realizowane poprzez jedno ze złącz USB-Cz funkcjonalnością Thunderbolt Type-C (w takim przypadku wymagane jest dostarczenie przejściówki z USB-C do RJ45 – gniazdo),
 - c) Bluetooth 5.2.
- 8) Bateria: nie mniej niż 86Wh;
- 9) Waga: nie więcej niż 2,20 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. 720p z funkcją IR,

- e) zintegrowany czytnik linii papilarnych,
- f) dedykowany zasilacz z wtyczką USB Type-C z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL,
- g) wbudowany układ zabezpieczający TPM (Trusted Platform Module) lub równoważny,
- 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 włączenia/wyłączenia/restart komputera poprzez TCP/IP,
 - iii. zdalnego diagnozowania - zdalna konsola tekstowa do BIOSu i konsola graficzna (KVM),
 - iv. obsługi modułu TPM,
 - v. zdalnej konfiguracji BIOS, zdalnego update BIOS,
 - vi. zdalnego monitorowania stanu komponentów komputera – m.in. CPU, pamięć, dysk itp.,
 - vii. możliwości zdalnej blokady komputera w przypadku kradzieży. Jedynym warunkiem jest podłączenie komputera do sieci komputerowej oraz do zasilania.

- 11) System operacyjny: Licencja na system Windows 10 (lub 11) Professional PL 64-bit lub równoważny;
- 12) Wsparcie producenta dla następujących systemów operacyjnych:
 - a) Microsoft Windows 11 Pro 64-bit,
 - b) Ubuntu w wersji min. 20.04 LTS 64-bit,
 - c) Red Hat Enterprise Linux w wersji min. 8.6.
- 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.

6.1.2. Monitor

Jeden monitor opisany w punkcie 6.4

6.1.3. Stacja dokująca

Jedna stacja dokująca opisana w punkcie 6.5

6.1.4. Zestaw klawiatura z myszą

Jeden zestaw klawiatura z myszą Typ A opisany w punkcie 6.6

6.2. Stacja Zarządzania Typ 2

Pojedyncza Stacja Zarządzania Typ 2 składa się z następujących części składowych:

6.2.1. Jednostka główna spełniająca poniższe wymagania:

- 1) Wyświetlacz: 15,6" cala, rozdzielczość min. 1920x1080, gama barw min 72% sRGB, jasność min. 400 nit, o niskiej emisji światła niebieskiego, z powłoką przeciwoodblaskową;
- 2) Procesor: zgodny z x64, posiadający co najmniej 10 fizycznych rdzeni, w dwóch klasach wydajności (co najmniej 2 rdzenie zapewniające wydajność i co najmniej 8 rdzeni energooszczędnych), co najmniej 12 wątków. Zaprojektowany do pracy w mobilnych stacjach roboczych (pobór mocy w podstawowym trybie pracy nie więcej niż 15W, w trybie turbo nie więcej niż 55W), posiadający min. 12MB cache, osiągający wydajność minimum: 13300 punktów Passmark CPU Mark w teście wydajności Pass Mark Performance Test (stan na 25.10.2022) pracujący z minimalną częstotliwością w trybie turbo dla rdzeni energooszczędnych 3,60GHz oraz dla rdzeni zapewniających wydajność 4,80GHz;
- 3) Pamięć RAM: nie mniej niż 32 GB, min. DDR4;
- 4) Dysk twardy: nie mniej niż 1TB w technologii M.2 SSD PCIe x4 NVMe Class 40;
- 5) Zintegrowane porty (co najmniej):
 - a) min. 2x Port Thunderbolt 4 Type-C z obsługą standardu Display Port/ USB 4 / Power Delivery,
 - b) min. 2x USB 3.2 Gen 1 Type-A w tym co najmniej jeden z funkcją PowerShare,
 - c) zintegrowany czytnik kart microSD/mSDHC/mSDXC,
 - d) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm,
 - e) min. 1x HDMI 2.0,
 - f) wbudowane gniazdo czytnika kart SmartCard Reader,
 - g) wbudowany czytnik kart SmartCard Reader/NFC.
- 6) Komunikacja:
 - a) Wi-Fi 6 dwuzakresowa zgodna z co najmniej IEEE 802.11 ax/ac/a/b/g/n,
 - b) 1x LAN 10/100/1000 Ethernet wbudowana lub realizowana poprzez Thunderbolt Type-C (w takim przypadku wymagane jest dostarczenie przejściówki z USB-C do RJ45 – gniazdo),
 - c) Bluetooth 5.2;
- 7) Bateria: nie mniej niż 56Wh z Express Charge (wbudowana w obudowę);
- 8) Waga: nie więcej niż 1,8 kg;
- 9) Dodatkowe wymagania:
 - a) klawiatura: QWERTY, podświetlana,
 - b) Touchpad,
 - c) co najmniej dwa wbudowane głośniki oraz min. dwa mikrofony,
 - d) wbudowana kamera o rozdzielczości min. 720p z funkcją IR,
 - e) dedykowany zasilacz z wtyczką USB Type-C z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL
 - f) wbudowany układ zabezpieczający TPM (Trusted Platform Module) lub równoważny,
 - g) 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 graficzna (KVM),
- iv. obsługi modułu TMP,
- v. zdalnej konfiguracji BIOS, zdalny update BIOS,
- vi. zdalnego monitorowania stanu komponentów komputera – m.in. CPU, pamięć, dysk itp.,
- vii. możliwości zdalnej blokady komputera w przypadku kradzieży. Jedynym warunkiem jest podłączenie komputera do sieci komputerowej oraz do zasilania.

- 10) System operacyjny: Licencja na system Windows 10 (lub 11) Professional PL 64-bit lub równoważny;
- 11) Wsparcie producenta dla następujących systemów operacyjnych:
- a) Microsoft Windows 11 Pro 64-bit,
 - b) Ubuntu w wersji min. 20.04 LTS 64-bit.
- 12) Bezpłatne oprogramowanie do automatycznej diagnostyki z funkcją przewidywania usterek dysków twardej 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.

6.2.2. Monitor

Jeden monitor opisany w punkcie 6.4

6.2.3. Stacja dokująca

Jedna stacja dokująca opisana w punkcie 6.5

6.2.4. Zestaw klawiatura z myszą

Jeden zestaw klawiatura z myszą Typ A opisany w punkcie 6.6

6.3. Stacja Zarządzania Typ 3

Pojedyncza Stacja Zarządzania Typ 3 składa się z następujących części składowych:

6.3.1. Jednostka główna spełniająca poniższe wymagania:

- 1) Wyświetlacz: min. 16,2" cala, rozdzielczość min. 3456x2234, o jasność min. 1000 nit na całej powierzchni ekranu, kontraście min. 1 000 000:1 z funkcją dopasowania temperatury barw wyświetlacza do panującego oświetlenia;
- 2) Funkcję procesora oraz układu graficznego pełni system jednoukładowy (SoC), w którego skład wchodzi:

- a) co najmniej 10 fizycznych rdzeni, w dwóch klasach wydajności (co najmniej 8 rdzeni zapewniające wydajność i co najmniej 2 rdzenie energooszczędne),
 - b) wbudowany procesor graficzny z co najmniej 32 rdzeniami,
 - c) wbudowany co najmniej 16 rdzeniowy system wspomagający proces uczenia maszynowego,
- 3) zunifikowana pamięć RAM o pojemności co najmniej 64 GB;
- 4) Dysk twardy: nie mniej 2TB w technologii SSD;
- 5) Karta graficzna umożliwiająca jednocześnie wyświetlanie obrazu w pełnej natywnej rozdzielczości na wbudowanym wyświetlaczu oraz obsługę dwóch wyświetlaczy zewnętrznych o rozdzielczości 6K przy 60Hz każdy;
- 6) Zintegrowane porty (co najmniej):
- a) min. 3x gniazda Thunderbolt 4 (USB-C) z obsługą:
 - i. Display Port,
 - ii. USB 4 (do 40Gb/s),
 - iii. Power Delivery (ładowania),
 - iv. Thunderbolt 4 (do 40Gb/s).
 - b) Gniazdo HDMI
 - c) Gniazdo na kartę SDXC
 - d) magnetyczne złącze do zasilania
 - e) złącze słuchawkowo-mikrofonowe – Jack 3,5 mm.
- 7) Komunikacja:
- a) Wi-Fi dwuzakresowa zgodna z co najmniej IEEE 802.11 ax/ac/a/b/g/n,
 - b) 1x LAN 10/100/1000 Ethernet wbudowana lub realizowana poprzez jedno z gniazd Thunderbolt Type-C za pomocą dedykowanej przez producenta przejściówki Thunderbolt/USB-C na RJ-45 gniazdo, w takim przypadku należy taką przejściówkę dostarczyć.
 - c) Bluetooth min. 5.0.
- 8) Bateria: nie mniej niż 100Wh zapewniające min. 14 godzin bezprzewodowego przeglądania Internetu;
- 9) Zasilacz: dedykowany przez producenta stacji zarządzającej o mocy min. 140W z gniazdem USB Type-C wraz z dedykowanym kablem USB Type-C – magnetyczne złącze do zasilania o długości 2 metrów. Zasilacz musi poprawnie pracować w zakresie od 100V do 240V z częstotliwością pracy od 50Hz do 60Hz oraz umożliwiać podłączenie do zasilania z gniazdek używanych na terenie PL bez dodatkowych przejściówek lub adapterów
- 10) Waga: nie więcej niż 2,20 kg;
- 11) Dodatkowe wymagania:
- a) klawiatura: QWERTY, podświetlana,
 - b) gładzik z obsługą siły nacisku oraz obsługą gestów Multi-Touch,
 - c) co najmniej sześć wbudowanych głośników z układem min. trzech mikrofonów,
 - d) obsługa przestrzennego dźwięku stereo oraz Dolby Atmos,
 - e) wbudowana kamera HD o rozdzielczości min. 1080p,
 - f) zintegrowany czytnik linii papilarnych.
- 12) System operacyjny: Licencja na system macOS Monterey lub w nowszej wersji lub równoważny.
- 13) Wsparcie producenta dla następujących systemów operacyjnych:
- a) dla macOS woferowanej wersji,
- 14) Preferowany przez Zamawiającego kolor srebrny;

6.3.2. Monitor

Jeden monitor opisany w punkcie 6.4

6.3.3. Stacja dokująca

Jedna stacja dokująca opisana w punkcie 6.5

6.3.4. Zestaw klawiatura z myszą

Jeden zestaw klawiatura z myszą Typ B opisany w punkcie 6.7

6.4. Monitor

Kompatybilny ze stacjami zarządzania Typu 1-3 monitor LCD 27" 4K ze złączem USB-C o następującej parametrach technicznych:

- a) przekątna „27” – widoczna matryca min. 26.96" w formacie 16:9,
- b) rozdzielczość 3840 x 2160 (WQHD),
- c) matowa matryca IPS,
- d) kontrast min. 1000:1,
- e) czas reakcji monitora – 5 ms,
- f) kąty widzenia: 178° w pionie i poziomie,
- g) złącza (gniazda): min. 1x HDMI 2.0, min. 1x DisplayPort, min. 1x USB Type-C (z funkcją ładowania laptopa z mocą min. 65W),
- h) wbudowany hub USB: min. 2 x USB 3.0
- i) funkcje: funkcja obrotowego ekranu (PIVOT), regulacja wysokości (min. 110mm), regulacja kąta pochylecia (w zakresie min. -5/+20)
- j) dołączone przewody: 1 x kabel z wtyczkami DisplayPort, 1 x kabel z wtyczkami USB-C (Type-C),
- k) zasilanie – napięcie 100-240VAC,
- l) z monitorem musi zostać dostarczony przewód umożliwiającym zasilanie z gniazdek używanych na terenie PL,
- m) Waga z podstawką: nie więcej niż 7.5 kg.

6.5. Stacja dokująca

Stacja dokująca kompatybilna ze stacjami zarządzania Typu 1-3 podłączana poprzez Thunderbolt 4 Type-C za pomocą złącza USB Type-C. Musi być wyposażona co najmniej w następujące złącza (gniazda):

- a) 1x USB 3.2 Gen 2 Type-C,
- b) 3x USB 3.2 Gen 1 Type-A w tym co najmniej 1 z funkcjonalnością PowerShare
- c) 2x DisplayPort 1.4,
- d) 1x HDMI min. 2.0,
- e) 1x USB 3.2 Gen 2 Type-C 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 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. 0,8 m.

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 o mocy min. 90W (130W w przypadku podłączenia komputera producenta stacji dokującej) z obsługą napięcia 100-240VAC wraz z przewodem umożliwiającym zasilanie z gniazdek używanych na terenie PL. Wymagane jest aby dostarczane poprzez stację zasilanie było wystarczające do poprawnej pracy stacji zarządzania Typu 1-3 bez potrzeby podłączania ich do dodatkowego zasilania.

Dodatkowa wymagana poprawna obsługa: PXE Boot, Wake-On-LAN, Wake-On-Dock.

Stacja dokująca musi poprawnie współpracować z następującymi systemami operacyjnymi: Windows 10 i 11, Ubuntu min. 20.04, macOS (w przypadku systemu macOS nie jest wymagana obsługa funkcjonalności PXE Boot, Wake-On-LAN, Wake-On-Dock oraz praca z 3 monitorami w rozdzielczości 4k).

6.6. Zestaw klawiatura z myszą Typ A

- 1) Kompatybilny ze stacjami zarządzania Typu 1-3 zestaw klawiatury i myszy.
- 2) Musi posiadać następującą funkcjonalność:
 - a) zasilanie za pomocą baterii 2x AAA (klawiatura) oraz 1xAA (mysz) – poprawność pracy na jednym komplecie baterii 36 miesięcy,
 - b) możliwość jednoczesnego bezprzewodowe podłączenie do trzech różnych komputerów– jednego za pomocą odbiornika USB Type-A, pozostałych dwóch za pomocą Bluetooth. Przełączania pomiędzy poszczególnymi komputerami musi 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. 1000 dpi,
 - e) mysz musi posiadać co najmniej 7 przycisków,
 - f) poprawna współpraca z systemami: Microsoft Windows 10, Android, Apple macOS.
- 3) Do zestawu muszą zostać dołączone baterie w liczbie i modelu umożliwiającym poprawną pracę zestawu.

6.7. Zestaw klawiatura z myszą Typ B

Dedykowana przez producenta klawiatura oraz mysz bezprzewodowa do stacji zarządzania Typu 3 o następujących parametrach technicznych:

- 1) bezprzewodowa klawiatura z wydzielonym polem numerycznym:
 - a) układ klawiatury: angielski (międzynarodowy) lub angielski (amerykański),
 - b) wyposażona w oddzielny blok numeryczny,
 - c) dedykowane klawisze do obsługi systemu macOS oraz multimediiów,
 - d) komunikacja za pomocą Bluetooth,
 - e) wbudowane gniazdo Lightning służące do ładowania wbudowanego akumulatora oraz parowania myszy ze zgodnym komputerem,

Usunięte: <#>klawisze osadzone za pomocą mechanizmu nożycowego,¶

- f) parowanie klawiatury musi odbywać się automatycznie poprzez podłączenie za pomocą dostarczonego kabla do portu USB zgodnego komputera,
 - g) wbudowany akumulator wielokrotnego ładowania (jednorazowe naładowanie wystarcza na miesiąc pracy),
 - h) zintegrowany z klawiaturą czytnik linii papilarnych,
 - i) z klawiaturą musi zostać dostarczony przewód z USB Type-C na Lightning, który umożliwia ładowanie oraz parowanie ze zgodnym komputerem,
 - j) waga nie więcej niż 0,4 kg,
 - k) kolor identyczny jak myszy z pozycji 2).
 - l) Preferowany przez zamawiającego kolor szary lub biały
- 2) bezprzewodowa mysz:
- a) symetryczna budowa zapewniająca wygodną pracę osobom prawo i leworęcznym,
 - b) obsługa standardu Multi-Touch z obsługą gestów,
 - c) komunikacja za pomocą Bluetooth,
 - d) wbudowane gniazdo Lightning służące do ładowania wbudowanego akumulatora oraz parowania myszy ze zgodnym komputerem,
 - e) parowanie myszy musi odbywać się automatycznie poprzez podłączenie za pomocą dostarczonego kabla do portu USB Type-C zgodnego komputera,
 - f) wbudowany akumulator wielokrotnego ładowania (jednorazowe naładowanie wystarcza na miesiąc pracy),
 - g) z myszą musi zostać dostarczony przewód z USB Type-C na Lightning, który umożliwia ładowanie oraz parowanie ze zgodnym komputerem,
 - h) waga nie więcej niż 0,1 kg,
 - i) kolor identyczny jak klawiatury z pozycji 1).

Usunięte: <#>sensor laserowy,¶

6.8. Opis równoważności

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez Wykonawcę jako równoważne dla systemu operacyjnego Windows 10 (lub 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.

Poniżej opisano kryteria, jakie Zamawiający będzie stosował w celu oceny równoważności rozwiązania zaproponowanego przez Wykonawcę jako równoważne dla systemu operacyjnego macOS (Monterey lub nowszy) lub równoważny.

Przez równoważność Zamawiający rozumie konieczność:

1. zapewnienia przez system pełnej funkcjonalności jaką oferuje system macOS w minimalnej wskazanej przez Zamawiającego wersji,

-
2. dostępność dla systemu równoważnego tych aplikacji oraz oprogramowania, które są dostępne dla wskazanego przez Zamawiającego systemu macOS lub aplikacji i oprogramowań alternatywnych, zapewniających wszystkie te same funkcjonalności.

7. Wdrożenie systemu

W ramach wdrożenia każdej dostawy objętej zadaniem Wykonawca zobowiązany jest do:

- 1) realizacji planu wdrożenia zawartego w punkcie 7.1,
- 2) dostawy przedmiotu zapotrzebowania zgodnie z szczegółowym wykazem zamówienia opisanym w punkcie 10,
- 3) dostawy, instalacji i konfiguracji urządzeń wchodzących w skład poszczególnych zadań w lokalizacjach podanych w punkcie 7.2.2,
- 4) przeprowadzenie instruktażu dla pracowników Zamawiającego zgodnie z wytycznymi opisanymi w punkcie 8.

7.1. Ramowy plan wdrożenia

Lp.	Element wdrożenia	Dni robocze* (terminy maksymalne)
OPRACOWANIE DOKUMENTACJI TECHNICZNEJ		
1.	Wykonanie dokumentacji technicznej w zakresie dotyczącym danego podmiotu odbierającego, zgodnie z wytycznymi zawartymi w punkcie 7.4	30 dni od daty złożenia zapotrzebowania przez poszczególne podmioty odbierające ale przed rozpoczęciem dostawy
2.	Weryfikacja dokumentacji technicznej przez poszczególne podmioty odbierające	10 dni roboczych od dnia jej dostarczenia przez wykonawcę
3.	Naniesienie poprawek w dokumentacji technicznej przez wykonawcę zgodnie z wytycznymi poszczególnych podmiotów odbierających	5 dni roboczych od dnia zgłoszenia konieczności dokonania poprawek przez poszczególne podmioty odbierające
DOSTAWA I INSTALACJA SYSTEMU		
4.	Dostawa urządzeń i oprogramowania	30 dni roboczych od daty złożenia zapotrzebowania przez poszczególne podmioty odbierające
5.	Instalacja i konfiguracja obejmująca 3 etapy: 1. Instalacja urządzeń w szafach telekomunikacyjnych zlokalizowanych w obiektach poszczególnych podmiotów odbierających wraz z ułożeniem okablowania i podłączenie urządzeń do przełączników LAN i zasilania. 2. Instalacja i konfiguracja logiczna środowiska (serwery wraz z systemem do zarządzania, serwery dyskowe, platforma wirtualizacyjna wraz z modułami, przełączniki sieciowe). 3. Konfiguracja Systemu obejmująca konfigurację i	10 dni roboczych od daty dostarczenia urządzeń i oprogramowania do danego podmiotu odbierającego

	<p>uruchomienie platformy wirtualizacyjnej w sposób zgodny z wykonaną wcześniej przez wykonawcę i zaakceptowaną przez poszczególne podmioty odbierające Dokumentacją Techniczną.</p> <p>4. Przygotowanie i przeprowadzenie przez wykonawcę testów weryfikacyjnych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 7.6.1 z Części IV SWZ. Przygotowanie raportu podsumowującego wyniki testów</p>	
OPRACOWANIE DOKUMENTACJI POWYKONAWCZEJ		
6.	Wykonanie dokumentacji powykonawczej w zakresie dotyczącym danego podmiotu odbierającego przez wykonawcę zgodnie z wytycznymi w punkcie 7.5	10 dni roboczych po zakończeniu instalacji i konfiguracji Systemu u poszczególnego podmiotu odbierającego
7.	Weryfikacja dokumentacji powykonawczej przez poszczególne podmioty odbierające	5 dni roboczych od dnia jej dostarczenia przez wykonawcę
8.	Naniesienie poprawek do dokumentacji powykonawczej przez wykonawcę zgodnie z wytycznymi poszczególnych podmiotów odbierających	5 dni roboczych od dnia zgłoszenia konieczności dokonania poprawek przez poszczególne podmioty odbierające
WERYFIKACJA POPRAWNOŚCI INSTALACJI SYSTEMU (PRZEPROWADZENIE TESTÓW)		
9.	Przegotowanie przez wykonawcę planu testów akceptacyjnych i wydajnościowych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 7.6.2 i 7.6.3	5 dni roboczych po zakończeniu instalacji i konfiguracji Systemu u poszczególnego podmiotu odbierającego
10.	Weryfikacja planu testów akceptacyjnych i wydajnościowych przez poszczególny podmiot odbierający	3 dni robocze od dnia jego dostarczenia przez wykonawcę
11.	Naniesienie poprawek na planie testów akceptacyjnych i wydajnościowych przez wykonawcę zgodnie z wytycznymi u poszczególnego podmiotu odbierającego	3 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez poszczególny podmiot odbierający
12.	Wykonanie przez wykonawcę testów akceptacyjnych i wydajnościowych oraz wykonanie raportu podsumowującego wyniki testów wraz ze zgłoszeniem gotowości do testów odbiorczych	5 dni roboczych
13.	Przegotowanie przez wykonawcę planu testów odbiorczych instalacji i konfiguracji Systemu zgodnie z wytycznymi w punkcie 7.6.4	3 dni robocze od zgłoszenia gotowości do testów odbiorczych w odniesieniu do danego podmiotu odbierającego

14.	Weryfikacja planu testów odbiorczych przez poszczególne podmioty odbierający	3 dni robocze od dnia jego dostarczenia przez wykonawcę
15.	Naniesienie poprawek na planie testów odbiorczych przez Wykonawcę zgodnie z wytycznymi poszczególnego podmiotu odbierającego o	2 dni robocze od dnia zgłoszenia konieczności dokonania poprawek przez poszczególne podmioty odbierający
16.	Wykonanie testów odbiorczych przez wykonawcę i poszczególne podmioty odbierające i wykonanie przez wykonawcę raportu podsumowującego wyniki testów	3 dni robocze
17.	Podpisanie przez poszczególne podmioty odbierający protokołu zdawczo - odbiorczego przedmiotu zamówienia objętego danym zadaniem	1 dzień roboczy po pozytywnym zakończeniu testów odbiorczych u poszczególnego podmiotu odbierającego

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

7.2. Dostawa i instalacja

Wykonawca zobowiązany jest dostarczyć wszelkie urządzenia i oprogramowanie będące przedmiotem poszczególnego Zadania do lokalizacji wskazanych w punkcie **7.2.2** oraz wykonania ich instalacji w tej lokalizacji z uwzględnieniem warunków opisanych w punkcie **7.2.3**.

7.2.1. 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 urządzeń i oprogramowania, ich instalacji i konfiguracji w lokalizacjach podanych w punkcie **7.2.2**. 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 dostawą i montażem, jak i na trasie transportu materiałów oraz sprzętami 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 której 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 danego zadania (zapotrzebowania) jest usunięcie wszystkich odpadów powstałych w trakcie instalacji.
- 12) Wszystkie prace instalacyjne i wdrożeniowe muszą być wykonane w oparciu o najlepsze praktyki, standardy, najnowszą wiedzę w zakresie, który obejmuje zamówienie oraz obowiązujące przepisy.

7.2.2. Miejsce dostawy i instalacji poszczególnych Zadań.

Zamawiający wymaga, aby Wykonawca dostarczył oraz zainstalował komponenty w ramach danego zadania w następujących lokalizacjach:

- 1) Zadanie nr 1 – PW – Poznańskie Centrum Superkomputerowo-Sieciowe, Budynek Sal Technologicznych (BST) przy ul. Jana Pawła II 10 Poznań
- 2) Zadanie nr 2 – PCSS – Poznańskie Centrum Superkomputerowo-Sieciowe, Budynek Sal Technologicznych (BST) ul. Jana Pawła II 10 Poznań
- 3) Zadanie nr 3 – AGH – Akademia Górniczo-Hutnicza, 30-059 Kraków, ul. Czarnowiejska 74
- 4) Zadanie nr 4 – PG – Politechnika Gdańska, 80-233 Gdańsk, ul. G. Narutowicza 11/12, budynek WETI B – budynek nr 42 na mapie <https://campus.pg.edu.pl>, wjazd od strony ul. R. Traugutta przy skrzyżowaniu z ul. Siedlicką
- 5) Zadanie nr 5 – PWr – Politechnika Wrocławska, Budynek C3, ul. Z. Janiszewskiego 11/17, 50-372 Wrocław oraz Budynek C6, ul. C.K. Norwida 4/6, 50-373 Wrocław
- 6) Zadanie nr 6 – It – Instytut Łączności Państwowy Instytut Badawczy
lokalizacja A – ul. Swojczycka 38, 51-501 Wrocław
lokalizacja B – ul. Jaśkowa Dolina 15, 80-252 Gdańsk

7.2.3. Warunki instalacji dotyczące instalacji poszczególnych Zadań.

- 1) Zadanie nr 1 – PW
 - a) 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,
 - b) jeden kiosk składający się z 16 szaf teletechnicznych,
 - c) każda z szaf teletechnicznych posiada wymiary:
 - i) wysokość 47U,
 - ii) szerokość 80cm,
 - iii) głębokość 120cm,
 - iv) nośność szafy 1500kg,
 - v) nośność belek/profilu nośnych (pionowych) 1500kg,
 - vi) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”,
 - d) w każdej z szaf zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU,
 - e) 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,
 - f) sumaryczne chłodzenie na cały kiosk o mocy 200kW, realizowane za pomocą klimatyzatorów międzyrzędowych.
- 2) Zadanie nr 2 – PCSS
 - a) 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,
 - b) jeden kiosk składający się z 16 szaf teletechnicznych,
 - c) każda z szaf teletechnicznych posiada wymiary:
 - i) wysokość 47U,
 - ii) szerokość 80cm,
 - iii) głębokość 120cm,
 - iv) nośność szafy 1500kg,
 - v) nośność belek/profilu nośnych (pionowych) 1500kg,
 - vi) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”,
 - d) w każdej z szaf zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU,
 - e) 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,

- f) sumaryczne chłodzenie na cały kiosk o mocy 200kW, realizowane za pomocą klimatyzatorów międzyrzędowych.
- 3) Zadanie nr 3 – AGH
- a) miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu wyposażonym m.in. w podłogę techniczną z szachtami technicznymi oraz podwieszane korytka na potrzeby prowadzenia okablowania pomiędzy szafami, klimatyzację, system kontroli dostępu i monitoring,
 - b) szafy teletechniczne posiadające wymiary:
 - i) wysokość 42U,
 - ii) szerokość 80 cm,
 - iii) głębokość 100 cm,
 - iv) nośność szafy 1500 kg,
 - v) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”,
 - c) w każdej z szaf zasilanie z dwóch niezależnych torów, każdy z torów w postaci 2 listew zasilających PDU,
 - d) każda z listew PDU posiada:
 - i) zasilanie 3 fazowe,
 - ii) 18 gniazd okrągłych z bolcem 16A/230V,
 - e) sumaryczne chłodzenie na całą serwerownię (w której umieszczono 13 szaf) o mocy 60kW.
- 4) Zadanie nr 4 – PG
- a) miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu serwerowni na III piętrze budynku WETI-B wyposażonego w windę
 - b) szafy teletechniczne
 - i) wysokości 42U
 - ii) szerokości 80cm
 - iii) głębokość 120cm
 - iv) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”
 - v) listwy zasilające z gniazdami typu DIN49440 (Schuko) albo NF C61-314 (PL).
- 5) Zadanie nr 5 – PWr
- a) 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,
 - b) dwie szafy teletechniczne, z których każda posiada wymiary:
 - i) wysokość 47U,
 - ii) szerokość 80cm,
 - iii) głębokość 120cm,
 - iv) nośność szafy 1500kg,
 - v) nośność belek/profilu nośnych (pionowych) 1500kg,
 - vi) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”,

- c) w każdej z szaf zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU,
 - d) każda z listew PDU posiada:
 - i) zasilanie 3 fazowe,
 - ii) zabezpieczenie o łącznej mocy 32A na każdą szafę,
 - iii) 36 gniazd C13,
 - iv) 6 gniazd C19.
- 6) Zadanie nr 6 – Ił
- Lokalizacja A – ul. Swojczycka 38, 51-501 Wrocław
- a) miejsce instalacji urządzeń: Instytut Łączności PIB, ul. ul. Swojczycka 38, 51-501 Wrocław, budynek A, 1 piętro,
 - b) miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu wyposażonym w klimatyzację,
 - c) szafa teletechniczna posiadająca wymiary:
 - i) wysokość 42U,
 - ii) szerokość 80 cm,
 - iii) głębokość 100 cm,
 - iv) nośność szafy 1500 kg,
 - v) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”,
 - d) w każdej z szaf zasilanie z dwóch niezależnych torów, każdy z torów w postaci 2 listew zasilających PDU,
 - e) każda z listew PDU posiada:
 - i) zasilanie 3 fazowe,
 - ii) 18 gniazd okrągłych z bolcem 16A/230V,

Lokalizacja B - ul. Jaśkowa Dolina 15, 80-252 Gdańsk

- a) miejsce instalacji urządzeń: Instytut Łączności PIB, ul. Jaśkowa Dolina 15, 80-252 Gdańsk, budynek główny, 4 piętro, pokój 413.
- b) miejsce na instalację urządzeń w przeznaczonym do tego celu pomieszczeniu
- c) jeden kiosk składający się z 1 szafy teletechnicznej,
- d) Szafa teletechniczna posiada wymiary:
 - i) wysokość 47U,
 - ii) szerokość 80cm,
 - iii) głębokość 120cm,
 - iv) nośność szafy 1500kg,
 - v) nośność belek/profilu nośnych (pionowych) 1500kg,
 - vi) odległość między belkami umożliwiającą montaż urządzeń z uchwytami w rozstawie 19”,
- e) w każdej z szaf zasilanie z dwóch niezależnych torów w postaci 2 listew zasilających PDU, każda z listew PDU posiada:
 - i) zasilanie jednofazowe,
 - ii) Możliwe obciążenie: co najmniej 16A,
 - iii) minimum 10 gniazd C13,
 - iv) minimum 4 gniazda C19,

- f) sumaryczne chłodzenie o mocy minimum 12000 BTU (klimatyzator typu split).

7.2.4. Szczegółowe wymagania dotyczące dostawy i instalacji dla poszczególnych Zadań, które musi spełnić Wykonawca.

- 1) Zadanie nr 1 – PW
 - a) dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną,
 - b) wykonanie wszystkich niezbędnych połączeń, w tym także połączeń przewodów ochronnych,
 - c) wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - d) wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - e) wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz,
 - f) przełączniki sieciowe muszą być zainstalowane na tyle szafy patrząc od zewnątrz kiosku i przepływ powietrza musi odbywać się w kierunku od tyłu urządzenia do frontu (porty we/wy),
 - g) wszystkie połączenia kablowe muszą być prowadzone pod podłogą techniczną.
- 2) Zadanie nr 2 – PCSS
 - a) dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną,
 - b) wykonanie wszystkich niezbędnych połączeń, w tym także połączeń przewodów ochronnych,
 - c) wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - d) wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - e) wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz,
 - f) przełączniki sieciowe muszą być zainstalowane na tyle szafy patrząc od zewnątrz kiosku i przepływ powietrza musi odbywać się w kierunku od tyłu urządzenia do frontu (porty we/wy),
 - g) wszystkie połączenia kablowe muszą być prowadzone pod podłogą techniczną.
- 3) Zadanie nr 3 – AGH
 - a) dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną,
 - b) wykonanie wszystkich niezbędnych połączeń, w tym także połączeń przewodów ochronnych,

- c) wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - d) wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - e) wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz szafy do jej wnętrza,
 - f) wszystkie połączenia kablowe muszą być prowadzone pod podłogą techniczną lub w korytkach teletechnicznych przeznaczonych do tego celu.
- 4) Zadanie nr 4 – PG
- a) dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną,
 - b) wykonanie wszystkich niezbędnych połączeń, w tym także podłączeń przewodów ochronnych,
 - c) wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - d) wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa.
- 5) Zadanie nr 5 – PWr
- a) dostarczenia wszelkiego okablowania zasilającego niezbędnego do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną,
 - b) wykonania wszystkich niezbędnych połączeń zasilających oraz interfejsów zarządzania, w tym także podłączeń przewodów ochronnych,
 - c) wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - d) wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
 - e) wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wnętrza,
 - f) wszystkie połączenia kablowe muszą być prowadzone pod podłogą techniczną.
- 6) Zadanie nr 6 – IŁ
- a) dostarczenie wszelkiego okablowania zasilającego niezbędnego do realizacji zadania zgodnie z zapisami SWZ i Dokumentacją Techniczną,
 - b) wykonanie wszystkich niezbędnych połączeń, w tym także podłączeń przewodów ochronnych,
 - c) wszystkie dostarczone i instalowane urządzenia muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,

- d) wszystkie dostarczone i instalowane elementy okablowania muszą być jednoznacznie oznaczone zgodnie z uzgodnionym w ramach Dokumentacji Technicznej schematem nazewnictwa,
- e) wszystkie dostarczone urządzenia muszą być zainstalowane w sposób zapewniający przepływ powietrza z zewnątrz kiosku do wewnątrz,

7.3. Dokumentacja

- 1) Przygotowane przez Wykonawcę, w terminach wynikających ze szczegółowego planu wdrożenia danego zadania: Dokumentacja Techniczna, plany testów zgodnie z wytycznymi opisanymi w punkcie 7.6 oraz Dokumentacja Powykonawcza podlegają akceptacji Zamawiającego, odrębnie dla każdego z Zadań.
- 2) Zamawiający może zgłosić uwagi do dokumentów, o których mowa w ust. 1 powyżej, w terminach podanych w punkcie z 7.1 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 7.1, od dnia zgłoszenia uwag, natomiast Zamawiający nie później niż w terminie podanym w punkcie 7.1, 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 7.1 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: 7.3, 7.4 i 7.5.
- 6) Szczegółowe wytyczne dla testów zostały wskazane punkcie 7.6.
- 7) Wykonawca musi przygotować oddzielny zestaw dokumentów, o których mowa w ust. 1 powyżej, dla każdego z Zadań.

7.4. Dokumentacja Techniczna

Przed przystąpieniem do realizacji dostawy danego zadania przez Wykonawcę przez Zamawiającego musi zostać zaakceptowana dokumentacja techniczna dotycząca danego Zadania w celu weryfikacji poprawności koncepcji realizacji poszczególnego Zadania 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 szczegółowy plan wdrożenia uwzględniający ramowy plan wdrożenia opisany w punkcie 7.1, z dopuszczeniem dokonania zmian lub odchyień w stosunku do niego po uzyskaniu akceptacji Zamawiającego.
- 4) musi zawierać co najmniej:

- a) listę wymagań funkcjonalnych Zamawiającego,
- b) sposób realizacji wymagań funkcjonalnych,
- c) architekturę Systemu,
- d) schemat architektury wraz ze schematem przepływu danych między Komponentami,
- e) fizyczny i logiczny model połączeń poszczególnych Komponentów,
- f) aranżację poszczególnych elementów w szafach teletechnicznych,
- g) schemat nazewnictwa wszystkich dostarczonych elementów,
- h) schemat nazewnictwa wszystkich wykorzystywanych interfejsów,
- i) plany konfiguracji sieci w tym adresacji, portów itd. (IP design) wszystkich podłączonych do sieci Komponentów,
- j) architekturę połączeń wszystkich elementów sieciowych (co najmniej: adresacja IP, diagramy połączeń, sposób realizacji redundancji połączeń pomiędzy urządzeniami),
- k) plany instalacji urządzeń i podłączenia do sieci LAN i zasilania, w tym porty itd. (obwody prądowe),
- l) opis integracji, a w tym:
 - i. architektura i sposób zapewnienia zdalnego dostępu do poszczególnych Komponentów,
- m) listę wdrażanych Komponentów wraz z ich ilościami,
- n) dokumentację producentów wszystkich użytych Komponentów i elementów systemu (może być dostarczona w wersji elektronicznej),
- o) inne, wg uznania Wykonawcy.

7.5. Dokumentacja Powykonawcza

7.5.1. Wymagania

- 1) Do każdego wdrożonego Zadania musi zostać wykonana oddzielna Dokumentacja Powykonawcza.
- 2) Dokumentacja Powykonawcza musi być zgodna z Dokumentacją Techniczną opisaną w pkt. 7.4 i jeśli od niego odbiega powinien być załączony opis z czego ta różnica wynika.
- 3) Dokumentacja Powykonawcza musi zawierać szczegółowe procedury eksploatacyjne i utrzymaniowe, a także procedury zgłaszania do Wykonawcy awarii i problemów z Systemem w okresie gwarancji.
- 4) Dokumentacja Powykonawcza musi zawierać szczegółową konfigurację dostępu administracyjnych do Komponentów.
- 5) Dokumentacja Powykonawcza musi zawierać procedury zarządzania użytkownikami i ich uprawnieniami.
- 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 zawierać także:
 - 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 Zadania – co najmniej schemat logiczny i fizyczny połączeń, zestawienie użytych adresacji, konfiguracja urządzeń sieciowych,
 - e) dokumentację zarządzania Out-of-Band dostarczonymi urządzeniami – co najmniej schemat logiczny i fizyczny połączeń, zestawienie użytych adresacji, 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:
- a) szczegółowy model architektury Komponentów rozwiązania wraz z integracjami,
 - b) opis scenariuszy i raportów wszystkich testów,
 - c) szczegółowa architektura platformy wirtualizacyjnej wraz z jej modułami,
 - d) szczegółowa architektura dostarczonych serwerów dyskowych,
 - e) szczegółowa architektura bezpieczeństwa Systemu,
 - f) opis konfiguracji elementów Systemu zgodnie z wymaganiami z punktu **7.5.3**,
 - g) architektura, opis działania oraz parametry HA,
 - h) szczegółowa architektura i konfiguracja wszystkich przewidzianych integracji,
 - i) szczegółowy opis monitorowania, raportowania i automatyzacji Komponentów wchodzących w skład Systemu,
 - j) szczegółowy opis i konfiguracja Systemu w zakresie dostępu administracyjnego, uwierzytelniania i autoryzacji dla użytkowników,
 - k) instrukcje administratora systemu (co najmniej na poziomie zarządzania i używania, oraz analizy możliwych problemów).
- 10) Opis konfiguracji elementów Systemu
- Dokumentacja Powykonawcza w zakresie konfiguracji musi obejmować wszystkie elementy wdrożone, zainstalowane w ramach realizacji przedmiotu poszczególnego Zadania. Minimalny zestaw wymaganych danych konfiguracyjnych obejmuje:
- a) model urządzenia, parametry sprzętowe (np. kontrolery, półki dyskowe, dyski, przełączniki, wkładki, itp.), konfigurację serwerów dyskowych (grupy dyskowe, zasoby dyskowe itp.), sposób podłączenia 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,
 - j) zestawienie wszystkich ustawionych haseł do elementów Systemu w formie zakodowanego pliku.
- 11) Do Dokumentacji Powykonawczej musi być załączony raport z testów wykonanych po realizacji wdrożenia.

7.6. Wytyczne do testów

Procedura testowa musi być niezależna dla każdego Zadania.

Proces testowania Systemu związany z wdrożeniem i ewentualnymi zmianami w Systemie składa się z 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.

7.6.1. 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 projektu architektury.

7.6.2. Testy akceptacyjne (podstawowe i niezawodnościowe)

Nazwa testów	Testy akceptacyjne (podstawowe i niezawodnościowe)
--------------	--

Cel testów	weryfikacja poprawności działania poszczególnych elementów dostarczonego Zadania
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 poszczególnych Komponentów dostarczonego w ramach Zadania.

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 w ramach danego Zadania.

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 narzędzenia 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 zarządzania serwerami,
- 14) weryfikacja wszystkich elementów serwerów dyskowych i ich parametrów,

- 15) weryfikacja możliwości zarządzania serwerów dyskowych,
- 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.

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 w ramach danego Zadania.

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 przypisaną polityką odporności na awarię minimum jednego hosta,
- 2) symulacje awarii dysku z danymi 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.

7.6.3. 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.

7.6.4. Testy odbiorcze

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

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

- 1) Zgłaszając Zamawiającemu gotowość Systemu do 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: 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 kopii zapasowej w środowisku:
 - a) wykonanie i odtworzenie kopii maszyny wirtualnej
- 6) dostępności danych dla serwera dyskowego:
 - 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
 - c) skasowanie wirtualnej maszyny i odtworzenie z ostatniej kopii zapasowej.

7.7. Odbiory

Odbiór oznacza przeprowadzenie testów odbiorczych oraz potwierdzenie protokołem zdawczo – odbiorczym danego zadania (zapotrzebowania) 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 Zadania.

Ponadto w protokole zdawczo -odbiorczym ostatniego chronologicznie zadania potwierdzone będzie odbycie się wszystkich wymaganych instruktaży.

8. Instruktaż

8.1. Wstęp

W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do przeprowadzenia instruktaży zgodnie z przedstawionymi poniżej wymaganiami Zamawiającego. Instruktaże będą przeprowadzane w blokach tematycznych opisanych w pkt. 8.3 jako wspólne instruktaże dla wszystkich podmiotów odbierających. Szczegółowy zakres tematyczny jest zawarty w pkt. 8.2.10

8.2. Zbiór wymagań dla instruktaży

- 1) Wykonawca zapewni materiały instruktażowe w języku polskim lub angielskim dla wszystkich uczestników instruktaży (prezentacje, książki/podręczniki, ćwiczenia).
- 2) Maksymalna liczba osób w danej grupie nie przekroczy 30 osób.
- 3) Wykonawca przeprowadzi instruktaże w formie praktycznych zadań, istnieje możliwość przeprowadzenia ich na dostarczonym i wdrożonym środowisku będącym przedmiotem tego postępowania. Nie może dojść do sytuacji, że wdrożone środowisko po przeprowadzeniu instruktażu będzie нефunkcjonalne.
- 4) Instruktaże muszą być przeprowadzone przez instruktorów posiadających certyfikaty poświadczające ich wiedzę, wydane przez producenta/producentów dostarczonego Systemu lub poszczególnych Komponentów/modułów tego Systemu.
- 5) Instruktaż musi być przeprowadzony w trybie zdalnym na platformie zapewnionej przez Wykonawcę (przez system wideokonferencyjny).
- 6) Nie dopuszcza się instruktażu w formie szkolenia typu „e-learning”.
- 7) Termin instruktażu musi zostać ustalony z Zamawiającym. Wykonawca musi zaproponować co najmniej 3 terminy instruktażu.
- 8) Zakres poszczególnych instruktaży musi być uzgadniany i zaakceptowany przez Zamawiającego.
- 9) W każdym instruktarzu należy uwzględnić czas na pytania od uczestników.
- 10) Szczegółowy zakres merytoryczny instruktaży:
 - a) instruktaż wstępny:
 - i) omówienie architektury Systemu, w tym na podstawie dokumentacji wykonawczej m.in.
 - (1) architektury serwerów i serwerów dyskowych
 - (2) architektury platformy wirtualizacyjnej wraz z wszystkimi jej modułami
 - (3) architektury serwera dyskowego
 - (4) architektury urządzeń sieciowych
 - (5) architektury wdrożonego systemu wirtualizacyjnego
 - (6) podstawowej funkcjonalności wdrożonego systemu wirtualizacyjnego w szczególności w zakresie:
 - (a) tworzenie alertów, raportów i widoków
 - (b) omówienie procesów tworzenia i odzyskiwania kopii zapasowej
 - (c) omówienie procesu odzyskania środowisk po awarii
 - (d) aspekty związane z monitorowaniem infrastruktury Systemu
 - (e) aspekty związane z platformą wirtualizacyjną wraz z wszystkimi jej modułami
 - (f) aspekty związane z zarządzaniem wirtualizacją zasobów obliczeniowych

- (g) aspektów związanych z serwerami dyskowymi
- (h) aspektów związanych z urządzeniami sieciowymi
- ii) techniczne omówienie architektury wdrożonego Systemu
- iii) zarządzanie infrastrukturą serwerów fizycznych i zwirtualizowanych
- iv) zarządzanie platformą wirtualizacji obejmującą wszystkie jej moduły dostarczone w ramach postępowania
- v) omówienie i zarządzanie procesami tworzenia i odzyskiwania kopii zapasowej
- vi) omówienie i zarządzanie procesami odzyskania środowisk po awarii
- vii) omówienie i zarządzanie serwerem dyskowym
- viii) zarządzanie monitorowaniem warstwy wirtualizacji wraz z serwerami fizycznymi
- ix) aspekty związane z zarządzaniem oprogramowaniem monitorującym wirtualizację
- x) zarządzanie użytkownikami, rolami, poziomami dostępu.
- b) instalacja, konfiguracja i zarządzanie serwerami:
 - i) proces instalacji, konfiguracji, zarządzania serwerem,
 - ii) proces aktualizacji oprogramowania Komponentów serwerów,
 - iii) proces aktualizacji oprogramowania zainstalowanego na serwerach,
 - iv) omówienie funkcjonalności systemu do zarządzania serwerem.
- c) implementacja i zarządzanie serwerem dyskowym, w tym ćwiczenia praktyczne z poniższej tematyki:
 - i) omówienie architektury serwera dyskowego,
 - ii) omówienie elementów składowych serwera dyskowego (sprzętowe i programowe składniki),
 - iii) omówienie konfiguracji serwera dyskowego,
 - iv) omówienie konfiguracji pod kątem odporności na awarie oraz wydajności,
 - v) omówienie protokołów dostępu i ich konfiguracji,
 - vi) omówienie udostępniania urządzeń blokowych przez protokół iSCSI,
 - vii) kopie migawkowe,
 - viii) „tiering” bloków danych pomiędzy dyskami,
 - ix) wymagania pracy całkowicie bez przestojów z zapewnieniem najwyższego poziomu trwałości danych,
 - x) redukcja danych (deduplikacja),
 - xi) naprawa po awarii sprzętowej,
 - xii) hot-spare lub przestrzeń nadmiarowa,
 - xiii) zabezpieczenie danych przed złośliwym oprogramowaniem szyfrującym,
 - xiv) gwarancja niezmienności danych,
 - xv) stosowanie wielu protokołów dostępu działających jednocześnie,
 - xvi) mechanizmy ochrony danych (synchronizacje, replikacje w wielu różnych topologiach) pomiędzy lokalizacjami i ich zastosowanie,
 - xvii) sposoby monitorowania serwera dyskowego,
 - xviii) diagnozowanie problemów i awarii,
 - xix) punkty zarządzania serwerem dyskowym,
 - xx) aktualizacja oprogramowania.
- d) instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz modułem oprogramowania do zarządzania klastrem wirtualizacyjnym, w tym ćwiczenia praktyczne z poniższej tematyki:
 - i) proces instalacji, konfiguracji, zarządzania oprogramowaniem do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz oprogramowaniem do zarządzania klastrem wirtualizacyjnym,

- ii) omówienie instalacji oraz konfiguracji i funkcjonalności konsoli graficznej do zarządzania maszynami wirtualnymi,
 - iii) opcje konfiguracji wirtualizatora i przełącznika sieciowego,
 - iv) konfiguracja wirtualizatora i przełącznika sieciowego w zakresie migracji maszyn wirtualnych w trakcie pracy, między serwerami,
 - v) omówienie koncepcji pamięci masowej i stosowania wirtualizacji,
 - vi) konfiguracja interfejsu zarządzania wirtualizatorem w serwerze, tworzenie magazynów danych,
 - vii) omówienie mechanizmów rozkładania obciążenia i migracji maszyn wirtualnych i plików maszyn wirtualnych,
 - viii) konfiguracja automatyzacji migracji maszyn wirtualnych,
 - ix) omówienie koncepcji i narzędzia do aktualizacji środowiska,
 - x) wykonanie aktualizacji serwerów,
 - xi) profilowanie serwerów dla uproszczenia konfiguracji,
 - xii) konfiguracja wysokiej dostępności wirtualizacji poprzez klastry,
 - xiii) tworzenie szablonów maszyn wirtualnych i bibliotek scenariuszy,
 - xiv) tworzenie, modyfikacja, przenoszenie, usuwanie maszyn wirtualnych,
 - xv) wdrażanie maszyn wirtualnych z szablonów,
 - xvi) klonowanie maszyn wirtualnych,
 - xvii) monitorowanie zasobów maszyn wirtualnych,
 - xviii) konfiguracja i przywracanie z kopii zapasowej głównej konsoli zarządzającej,
 - xix) konfiguracja przekazywania logów do zewnętrznych systemów np. SIEM,
 - xx) konfiguracja wysokiej dostępności dla głównej konsoli zarządzającej,
 - xxi) monitoring poprzez konsolę zarządzającą,
 - xxii) konfiguracja wbudowanego serwera zapory sieciowej w oprogramowaniu do zarządzania klastrem wirtualizacyjnym,
 - xxiii) konfiguracja uwierzytelniania użytkowników logujących się do oprogramowania zarządzającego klastrem wirtualizacyjnym w oparciu o domenę Microsoft Active Directory lub Open LDAP.
- e) instalacja, konfiguracja i zarządzanie modulem oprogramowania do wirtualizacji sieci, w tym ćwiczenia praktyczne z poniższej tematyki:
- i) sposoby instalacji, konfiguracji i zarządzania modulem oprogramowania do wirtualizacji sieci
 - ii) wyjaśnienie i omówienie tematyki: logiczne przełączanie, logiczny routing, usługi sieciowe i bezpieczeństwo, mikro-segmentacja, zapory ogniowe i inne komponenty,
 - iii) wyjaśnienie funkcjonalności, wymagań technicznych i ograniczeń w module oprogramowania do wirtualizacji sieci
 - iv) przeprowadzenie laboratorium z zakresu praktycznych zadań na temat instalacji, konfiguracji i zarządzania modulem,
 - v) budowanie architektury sieci zdefiniowanej programowo,
 - vi) omówienie Komponentów i głównych funkcjonalności,
 - vii) omówienie kluczowych funkcji i zalet stosowania,
 - viii) sposoby powoływania środowisk testowych jako kopii środowiska produkcyjnego,
 - ix) omówienie procesu wdrażania i konfiguracji infrastruktury sieci zdefiniowanej programowo,
 - x) omówienie wymagań na sieć podkładową,
 - xi) omówienie metod łączenia sieci zdefiniowanej programowo z siecią podkładową i usługami takimi jak Firewall, LoadBalancer, itp.,

- xii) omówienie konfiguracji logicznego przełączania i mostkowania warstwy 2,
 - xiii) omówienie wielopoziomowej architektury routingu i konfiguracji bramy IP,
 - xiv) omówienie zaawansowanych usług, takich jak VPN i równoważenie obciążenia, sposoby implementacji,
 - xv) omówienie bezpieczeństwa usług w sieci programowej poprzez stosowanie mikrosegmentacji, izolacja ruchu L2/VLAN,
 - xvi) omówienie bezpieczeństwa modeli zapór ogniowych w celu chronienia ruchu wschód-zachód i północ-południe,
 - xvii) omówienie zaawansowanego wymuszania bezpieczeństwa w połączeniu ze środowiskiem produktów podmiotów trzecich,
 - xviii) omówienie konfiguracji kontroli dostępu opartej na rolach,
 - xix) sposoby zabezpieczania usług między centrami danych,
 - xx) sposoby monitorowania sieci zdefiniowanej programowo,
 - xxi) diagnostyka problemów z siecią podkładową,
 - xxii) sposoby aktualizacji oprogramowania.
- f) instalacja, konfiguracja i zarządzanie urządzeniami sieciowymi:
- i) omówienie architektury w tym w szczególności architektury „leaf-spine”,
 - ii) omówienie topologii połączeń między przełącznikami,
 - iii) omówienie metod zarządzania przełącznikami, w tym interfejsu CLI,
 - iv) omówienie kluczowych aspektów i zalet architektury „leaf-spine”,
 - v) omówienie oraz konfiguracja i zarządzanie przełącznikami w architekturze „leaf-spine” na poziomie warstwy IP,
 - vi) omówienie oraz konfiguracja i zarządzanie trybem wysokiej dostępności przełączników (ang. HA),
 - vii) wykonanie praktycznych ćwiczeń laboratoryjnych z rozwiązywania problemów, przypadków awarii oraz metodologia rozwiązywania problemów,
 - viii) sposoby monitorowania przełączników,
 - ix) diagnozowanie problemów i awarii,
 - x) aktualizacja oprogramowania,
 - xi) bieżące prace administracyjne na przełącznikach.
- g) pozostałe
- i) koncepcja działania Systemu:
 - (1) źródła danych i typy obiektów w Systemie,
 - (2) użyte protokoły i interfejsy dostępu oraz ich konfiguracja,
 - (3) systemy klienckie,
 - (4) przepływ danych w poszczególnych warstwach,
 - (5) zabezpieczenie danych w kolejnych warstwach.
 - ii) procesy archiwizacyjne:
 - (1) omówienie procesu archiwizacji i przywracania danych w zależności od źródła danych, użytych protokołów i interfejsów,
 - (2) omówienie automatycznych i półautomatycznych procesów archiwizacji danych,
 - (3) omówienie bieżących zadań dla administratorów,
 - (4) omówienie zadań z perspektywy poszczególnych konsol zarządzających,
 - (5) omówienie polityk sterujących przenoszeniem danych pomiędzy warstwami,
 - (6) tworzenie i modyfikacja polityk.
 - iii) utrzymanie i konserwacja Systemu:
 - (1) procedura całkowitego wyłączenia Systemu i jej wpływ na systemy produkcyjne,
 - (2) przywracanie Systemu po awarii – omówienie scenariuszy,

- (3) weryfikacja poprawności pracy Systemu,
 - (4) analiza obciążenia Systemu,
 - (5) analiza zajętości Systemu, obowiązki administratorów w codziennym utrzymaniu Systemu,
 - (6) integracja z zewnętrznymi systemami monitorowania.
 - iv) rozwiązywanie problemów:
 - (1) sposoby poszukiwania przyczyn problemów w komunikacji sieciowej
 - (2) praktyczne ćwiczenia zapewniające pozyskanie zaawansowanej wiedzy i umiejętności w zakresie monitorowania, diagnostyki i rozwiązywania problemów
 - v) rozwój i planowanie zmian:
 - (1) omówienie skalowalności Systemu,
 - (2) omówienie zakresu elastyczności w poszczególnych punktach Systemu,
 - (3) przedstawienie dobrych praktyk w zakresie rozbudowy Systemu i zmian w Oprogramowaniu,
 - (4) omówienie wsparcia dla procesu wymiany technologii (technology refresh).
 - vi) gwarancja i utrzymanie:
 - (1) przedstawienie obowiązków Wykonawcy,
 - (2) omówienie procesu zgłaszania problemów.
- 11) Szczegółowy zakres instruktaży zawiera obszary, które muszą zostać zawarte w trakcie instruktażu, jednakże Zamawiający dopuszcza ich modyfikację przez Wykonawcę po uzgodnieniu tego z Zamawiającym i uzyskaniu od niego akceptacji zmiany zakresu.

8.3. Zestawienie instruktaży wraz z czasem trwania

Tabela długości poszczególnych instruktaży. Jako podstawową jednostkę czasu trwania instruktażu przyjmuje się jeden dzień (po 8 godzin zegarowych)

Lp.	Zakres	Czas trwania
1	instruktaż wstępny	2 dni
2	instalacja, konfiguracja i zarządzanie serwerami	1 dzień
3	implementacja i zarządzanie serwerem dyskowym	1 dzień
4	instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji zasobów serwerowych i ich mocy obliczeniowej oraz modułem oprogramowaniem do zarządzania klastrem wirtualizacyjnym	2 dni
5	instalacja, konfiguracja i zarządzanie modułem oprogramowania do wirtualizacji sieci	4 dni
6	instalacja, konfiguracja i zarządzanie urządzeniami sieciowymi	4 dni
7	pozostałe	1 dzień

9. Gwarancja

9.1. 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 wynosi 7 (siedem) lat i rozpoczyna swój bieg od daty podpisania protokołu zdawczo - odbiorczego danego zadania za wyjątkiem okresu gwarancji na dostarczone stacje zarządzania, który musi być zgodny z minimalnymi warunkami opisanym w punkcie **9.2.15**.
- 3) Zamawiający może dokonywać 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 danego zadania, z zastrzeżeniem, że rozbudowa została dokonana zgodnie z zaleceniami/wytycznymi producenta/producentów rozbudowywanych elementów Systemu.
- 4) Gwarancja Wykonawcy 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 niegorszych 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 Systemów,
 - 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 obowiązującą 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, nieekspozowany 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.

9.2. Opis usługi Gwarancji

9.2.1. Diagnostyka i rozwiązywanie problemów

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

9.2.2. 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.

Usunięte: .

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.

Usunięte: <#>brak możliwości realizacji usług.¶

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.

9.2.3. 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

Usunięte: 1

Usunięte: a

Usunięte: 4

Usunięte: y

Usunięte: 2

Usunięte: 8

Usunięte: y

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

9.2.4. 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 dostępu do systemu zgłoszeń problemowych Wykonawcy zostaną przekazane Zamawiającemu w trybie roboczym.

- 7) Strony, w trakcie trwania usługi gwarancji, mogą umówić się na integrację między systemami zgłoszeń problemowych Wykonawcy i Zamawiającego. Szczegóły zostaną uzgodnione w trybie roboczym.

9.2.5. 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.

9.2.6. 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.

9.2.7. 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 zapewni 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 przekaze 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.

9.2.8. 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 **9.2.3**, 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.

9.2.9. 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 **pkt. 9.2.3**
- 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.

9.2.10. 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 9.2.3.

9.2.11. 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 9.2.4, 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 zgłoszenia analogicznego Problemu, zostanie ono zarejestrowane przez Wykonawcę pod innym numerem zgłoszenia.

9.2.12. 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,
 - 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

9.2.13. Dostarczanie i wsparcie w instalacji Oprogramowania

W zakresie gwarancji Wykonawca zapewni 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 całym okresie gwarancji, Wykonawca zapewni 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 dotyczące 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

9.2.14. Szczegółowe wymagania gwarancji dotyczące elementów Systemu, z wyłączeniem stacji zarządzania

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 wygaśnięciu 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 możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta (numer krajowy dostępny z całego terytorium Polski),
- 7) zagwarantowana możliwość 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.

9.2.15. Szczegółowe wymagania gwarancji dotyczące Stacji Zarządzania

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

Przedmiot Zamówienia	Czas reakcji (dni)	Czas naprawy/wymiany (dni)	Okres gwarancji (miesiące)
1	2	3	4
Stacja zarządzania Typ 1: – jednostka główna – monitor – zestaw klawiatura mysz Typ A – stacja dokująca	1 dzień roboczy od zgłoszenia	Następny dzień roboczy od zgłoszenia jednostka główna, 2 dni robocze od zgłoszenia pozostałe elementy	60 miesięcy
Stacja zarządzania Typ 2: – jednostka główna – monitor – zestaw klawiatura mysz Typ A – stacja dokująca	1 dzień roboczy od zgłoszenia	Następny dzień roboczy od zgłoszenia jednostka główna, 2 dni robocze od zgłoszenia pozostałe elementy	60 miesięcy

Stacja zarządzania Typ 3: – jednostka główna – monitor – zestaw klawiatura mysz Typ B – stacja dokująca	1 dzień roboczy od zgłoszenia	10 dni roboczych od zgłoszenia jednostka główna i pozostałe elementy, 2 dni robocze od zgłoszenia monitor i stacja dokująca	36 miesięcy jednostka główna 60 miesięcy monitor i stacja dokująca 12 miesięcy pozostałe elementy
--	-------------------------------------	---	---

Przez czas „naprawy/wymiany” rozumie się czas liczony od wysłania zgłoszenia do dokonania skutecznej naprawy; albo wymiany wadliwego towaru na wolny od wad i dostarczenia sprzętu zastępczego;

Wymaganie dotyczące stacji zarządzania Typu 1, 2:

- 1) Gwarancja musi zapewniać ochronę mobilnej stacji zarządzania (mobilnego komputera) przed uszkodzeniem fizycznym spowodowanymi typowymi zdarzeniami mogącymi powstać z winy użytkownika końcowego, takimi jak: upuszczenie, zalanie, skok napięcia (przebiecie) 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 i jego 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 trzy lata.
- 4) Zamawiający wymaga zapewnienia możliwości sprawdzenia konfiguracji sprzętowej na dedykowanej do tego celu stronie producenta po podaniu numeru seryjnego urządzenia.

Wymaganie dotyczące wszystkich typów stacji zarządzania:

- 1) prawo do pobierania uaktualnień oprogramowania układowego oraz sterowników także po wygaśnięciu gwarancji na urządzenie,
- 2) 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,
- 3) 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.

