

OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zadania:

„#Cyberbezpieczna Gmina Libiąż” – zakup środków trwałych i wyposażenia IT do UM w Libiążu – serwer kopii/klaster wysokiej dostępności. NAS, dyski twarde do macierzy dyskowej.numer referencyjny: **ZP.271.5.11.2024**

Spis treści

1. SERWER KOPII ZAPASOWEJ – KLASTER WYSOKIEJ DOSTĘPNOŚCI	1
2. SERWER NAS – 3 SZT.	15
3. DYSKI TWARDE DO MACIERZY DYSKOWEJ (SERWERA NAS) – 3 KPL.	17
4. WYMAGANIA, TERMIN WYKONANIA ORAZ NAZWY I KODY DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA OKREŚLONE WE WSPÓLNYM SŁOWNIKU ZAMÓWIEŃ PUBLICZNYCH	18

1. Serwer kopii zapasowej – klaster wysokiej dostępności

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Obudowa	1. Obudowa Rack o wysokości max 1U. 2. Obudowa pozwalająca na montaż 10 dysków 2.5". 3. Możliwość instalacji dysków SAS/SATA/NVMe. Obudowa musi umożliwiać instalację 4 dysków NVMe równolegle z pozostałymi typami dysków.
Płyta główna	4. Płyta główna z możliwością zainstalowania minimum jednego procesora oferującego do 96 rdzeni oraz 196 rdzeni dla konfiguracji dwuprocesorowej. 5. Płyta główna musi umożliwiać instalacje minimum 24 kości pamięci DDR5 z możliwością wyskalowania pamięci do minimum 6TB
Procesor	6. Zainstalowany jeden procesor min. 16-rdzeniowy, min. 3.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 180 w teście SPECrate2017_int_base w konfiguracji jednoprocesorowej, dostępnym na stronie www.spec.org .
RAM	7. 256GB DDR5 RDIMM 4800MHz. 8. Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie korekcji błędów m.in. ECC, Address/Command Parity, Write/Read Data CRC, Patrol Scrubber.
Kontroler RAID	9. Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 00, 1, 5, 6, 10, 50 i 60, posiadający minimum 4GB cache
Dyski twarde	10. Zainstalowane: 10.1. 2x dysk SSD SATA o pojemności min. 1,92TB, Hot-Plug

Strona 1 z 19

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>10.2. 6x dysk HDD SAS 2.4TB</p> <p>11. Możliwość zainstalowania dwóch dysków M.2 SSD o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 1.</p>
Gniazda PCIe	12. 2x PCIe 4.0
Interfejsy sieciowe/FC/SAS	13. Min. 2 interfejsy sieciowe 10Gb wyposażone we wkładki (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	<p>14. 4 porty USB w tym min:</p> <p>14.1. 2 porty USB 3.0 z tyłu obudowy,</p> <p>14.2. 1 port USB 3.0 z przodu obudowy</p> <p>14.3. 1 wewnętrzny port USB 3.0</p> <p>15. 1 port VGA z tyłu obudowy</p> <p>16. 3 dedykowane, wbudowane porty umożliwiające zarządzanie serwerem, z czego co najmniej jeden umożliwiający połączenie z graficznym interfejsem zarządzającym, przynajmniej jeden port na przodzie obudowy umożliwiający połączenie za pomocą USB Type-C.</p> <p>17. Oferowany serwer musi być wyposażony w zestaw wskaźników oraz przycisków na przednim i tylnym panelu, umożliwiający łatwe monitorowanie stanu systemu oraz obsługę urządzenia. Wymagania obejmują następujące elementy:</p> <p>18. Przedni panel serwera</p> <p>18.1. Przyciski:</p> <p>18.1.1. Przycisk zasilania: Serwer musi posiadać przycisk umożliwiający włączanie i wyłączanie urządzenia.</p> <p>18.1.2. Przycisk identyfikacji urządzenia (UID): Serwer musi być wyposażony w przycisk identyfikacyjny, który umożliwia lokalizację serwera w środowisku z wieloma urządzeniami poprzez aktywację odpowiedniego wskaźnika.</p> <p>18.2. Wskaźniki:</p> <p>18.2.1. Wskaźnik zasilania: Oferowany serwer musi posiadać wskaźnik informujący o stanie zasilania, sygnalizujący tryby pracy, takie jak włączenie, wyłączenie oraz stan czuwania.</p> <p>18.2.2. Wskaźnik identyfikacji urządzenia (UID): Wskaźnik musi sygnalizować aktywację funkcji identyfikacji serwera, ułatwiając jego lokalizację.</p> <p>18.2.3. Wskaźnik stanu systemu: Serwer musi posiadać wskaźnik sygnalizujący ogólny stan systemu, wskazujący ewentualne błędy, ostrzeżenia lub stan gotowości.</p> <p>18.2.4. Wskaźniki aktywności dysków: Każdy dysk zamontowany w serwerze musi posiadać własny wskaźnik informujący o stanie aktywności oraz ewentualnych błędach dysku.</p> <p>19. Tylny panel serwera</p> <p>19.1. Wskaźniki portów sieciowych:</p> <p>19.1.1. Każdy port sieciowy musi być wyposażony w wskaźnik sygnalizujący stan połączenia (link status) oraz aktywność transmisji danych (data activity).</p> <p>19.2. Wskaźniki zasilaczy:</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>19.2.1. Serwer musi być wyposażony w redundantne zasilacze, a każdy z nich musi posiadać wskaźnik informujący o jego stanie pracy, sygnalizujący m.in. prawidłowe działanie, awarię lub odłączenie zasilania.</p> <p>20. Wymagania dodatkowe</p> <p>20.1. Wszystkie wskaźniki muszą być widoczne i czytelne zarówno z przodu, jak i z tyłu serwera, niezależnie od warunków oświetleniowych w centrum danych.</p> <p>20.2. Przyciski oraz wskaźniki muszą być opisane w dokumentacji serwera, a ich funkcje powinny być zgodne z najlepszymi praktykami rynkowymi, zapewniając łatwość obsługi oraz diagnostyki.</p>
Video	21. Zintegrowana karta graficzna z minimum 32MB pamięci osiągająca rozdzielczość min. 1920x1200 60Hz
Wentylatory	22. Redundantne
Zasilacze	23. Minimum dwa redundantne zasilacze o mocy minimum 900W z certyfikatem minimum Titanium.
Elementy montażowe	<p>24. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</p> <p>25. Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych</p>
Bezpieczeństwo	<p>26. Security panel chroniący przed nieautoryzowanym dostępem do dysków twardych.</p> <p>27. Moduł TPM 2.0</p> <p>28. Secure boot</p> <p>29. Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera.</p>
Moduł zarządzania	<p>30. Niezależny od zainstalowanego na serwerze systemu operacyjnego, moduł zarządzania, posiadająca dedykowany port Gigabit Ethernet RJ45.</p> <p>31. NC-SI</p> <p>32. Zarządzanie certyfikatami. Moduł musi obsługiwać szyfrowanie i wymianę certyfikatów SSL. Wymiana samych certyfikatów musi być możliwa z poziomu WebUI.</p> <p>33. Moduł musi umożliwiać import certyfikatu LDAP (Lightweight Directory Access Protocol).</p> <p>34. Wsparcie dla DCMI 1.5.</p> <p>35. Wsparcie dla IMPI 1.5 oraz 2.0.</p> <p>36. Moduł zarządzania musi posiadać certyfikację CC EAL4+.</p> <p>37. Wymagana jest funkcjonalność zarządzania diagnostyką błędów (FDM. Funkcjonalność musi obejmować zbieranie i analizę danych o błędach, diagnozowanie i lokalizowanie błędów, wczesne ostrzeganie o błędach oraz analizę kondycji urządzeń. Podczas rutynowej obsługi i konserwacji można wyświetlać informacje o wadliwych komponentach oraz związanych z nimi zdarzeniach historycznych. Wymagana funkcjonalność musi być możliwa do wyłączenia.</p> <p>38. Moduł musi oferować precyzyjne powiadomienia o niekrytycznych, nekorygowalnych błędach (UCE) w pamięci w sposób umożliwiający zlokalizowanie uszkodzonego modułu.</p> <p>39. Wymagana jest obsługa szczegółowych alarmów dotyczących dysków twardych, które mogą rozróżniać trzy typy alarmów: oprogramowania układowego dysku twardego, konfigurację i usterki fizyczne.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>40. Musi umożliwiać przeglądanie w formie graficznego modelu 3D rozkładu temperatury. Mapa temperatury musi umożliwić lokalizowanie anomalii związanych z temperaturą wewnątrz urządzenia w dowolnym jego punkcie.</p> <p>41. Moduł musi umożliwiać włączenie funkcji szyfrowania KVM i VNC (Virtual Network Console), które szyfrują dane przesyłane do zdalnej konsoli wirtualnej.</p>
BIOS	<p>42. Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności:</p> <p>42.1. Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.</p> <p>42.2. Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.</p> <p>42.3. Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu.</p> <p>42.4. Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware'u oraz zapewniać wsparcie dla aktualizacji zdalnych.</p>
System do zarządzania serwerem	<p>43. Oferowany serwer musi być wyposażony w zaawansowane oprogramowanie do zarządzania i monitorowania, które umożliwia centralne zarządzanie oraz optymalizację pracy serwera. Oprogramowanie musi spełniać następujące wymagania:</p> <p>44. Centralne zarządzanie serwerami</p> <p>44.1. Oprogramowanie do zarządzania serwerami musi zapewniać:</p> <p>44.1.1. Monitorowanie infrastruktury w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wydajności serwerów, stanu komponentów oraz zużycia zasobów, prezentując dane w formie graficznej.</p> <p>44.1.2. Automatyzacja aktualizacji: Musi wspierać zdalne i automatyczne aktualizowanie oprogramowania układowego oraz sterowników, z możliwością planowania aktualizacji.</p> <p>44.1.3. Diagnostyka i analiza stanu sprzętu: System musi umożliwiać analizę kondycji serwerów, gromadząc dane diagnostyczne i identyfikując potencjalne problemy przed ich wystąpieniem.</p> <p>44.1.4. Zarządzanie wieloma serwerami jednocześnie: Oprogramowanie musi umożliwiać zarządzanie co najmniej 50 serwerami z jednej platformy zarządzającej.</p> <p>45. Moduł zarządzania płytą główną</p> <p>45.1. Serwer musi być wyposażony w moduł zarządzania, który oferuje następujące funkcjonalności:</p> <p>45.1.1. Dostęp do zdalnej konsoli serwera: Moduł musi umożliwiać pełną kontrolę nad serwerem poprzez zdalny dostęp do konsoli, niezależnie od stanu systemu operacyjnego.</p> <p>45.1.2. Monitorowanie sprzętu: Moduł musi zapewniać monitorowanie parametrów sprzętowych, takich jak temperatura, prędkość wentylatorów, napięcia oraz stan kluczowych komponentów.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>45.1.3. Obsługa wirtualnych nośników: Moduł musi umożliwiać montowanie obrazów dysków zdalnie, co ułatwia instalację systemów operacyjnych oraz aktualizacje oprogramowania.</p> <p>45.1.4. Bezpieczne zarządzanie: Moduł musi wspierać szyfrowanie komunikacji oraz integrację z systemami uwierzytelniania, takimi jak LDAP, oraz zarządzanie certyfikatami.</p> <p>45.1.5. Wsparcie dla standardowych protokołów zarządzania: Moduł musi obsługiwać popularne protokoły zarządzania sprzętem, umożliwiając integrację z zewnętrznymi systemami zarządzania.</p> <p>46. System zarządzania zasobami serwera</p> <p>46.1. Serwer musi być wyposażony w oprogramowanie do zarządzania zasobami, które zapewnia:</p> <p>46.1.1. Monitorowanie obciążenia w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wykorzystania procesora, pamięci oraz przestrzeni dyskowej, prezentując dane w formie wykresów i raportów.</p> <p>46.1.2. Automatyczna optymalizacja zasobów: System musi posiadać funkcję automatycznego dostosowywania przydziału zasobów, aby maksymalizować wydajność serwera.</p> <p>46.1.3. Zarządzanie cyklem życia sprzętu: Oprogramowanie musi wspierać planowanie konserwacji, aktualizacje oprogramowania układowego oraz zarządzanie konfiguracją serwera.</p> <p>46.1.4. Integracja z zewnętrznymi systemami zarządzania: System musi obsługiwać standardowe interfejsy API, co umożliwia integrację z narzędziami do automatyzacji i zarządzania infrastrukturą.</p> <p>47. Oprogramowanie do zarządzania serwerem lokalnie i zdalnie</p> <p>47.1. Oferowane oprogramowanie musi umożliwiać zarządzanie serwerami zarówno lokalnie, jak i zdalnie, zapewniając:</p> <p>47.1.1. Automatyzację konfiguracji i monitorowania: Oprogramowanie musi umożliwiać automatyczną konfigurację serwerów, monitorowanie ich stanu oraz zarządzanie zasobami.</p> <p>47.1.2. Integrację z popularnymi platformami chmurowymi: Musi wspierać integrację z rozwiązaniami używanymi w środowiskach chmurowych, takimi jak narzędzia do wirtualizacji oraz systemy zarządzania centrami danych.</p> <p>47.1.3. Monitorowanie zużycia energii: Oprogramowanie musi oferować funkcje monitorowania zużycia energii oraz zarządzania profilami energetycznymi serwerów, co pozwala na optymalizację kosztów energii.</p> <p>48. Otwarte standardy zarządzania sprzętem</p> <p>48.1. Oprogramowanie musi wspierać otwarte standardy zarządzania sprzętem, takie jak nowoczesny interfejs API, który zapewnia:</p> <p>48.1.1. Zdalne zarządzanie sprzętem: API musi umożliwiać programistyczne zarządzanie serwerem, monitorowanie jego parametrów oraz automatyzację zadań administracyjnych.</p> <p>48.1.2. Bezpieczną komunikację: API musi wspierać szyfrowanie danych oraz integrację z narzędziami do zarządzania certyfikatami.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>48.1.3. Integrację z narzędziami do automatyzacji: API musi umożliwiać integrację z popularnymi narzędziami automatyzacji, takimi jak systemy zarządzania konfiguracją i orkiestracji.</p>
Wymagania dotyczące systemu diagnostycznego	<p>49. Oferowany serwer musi być wyposażony w zaawansowany system diagnostyczny, który zapewnia kompleksowe monitorowanie stanu sprzętu oraz precyzyjną diagnostykę problemów. Wymagane są następujące funkcjonalności:</p> <p>50. Funkcja diagnostyki błędów</p> <p>50.1. System musi zapewniać pełną funkcjonalność diagnostyki błędów, obejmującą:</p> <p>50.1.1. Zbieranie i analizę danych o błędach: Automatyczne gromadzenie danych diagnostycznych dotyczących kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde, zasilacze oraz wentylatory.</p> <p>50.1.2. Diagnozowanie i lokalizowanie usterek: System musi umożliwiać automatyczne wykrywanie i lokalizowanie usterek sprzętowych, wskazując precyzyjnie wadliwe komponenty.</p> <p>50.1.3. Wczesne ostrzeganie o błędach: Wymagane jest wsparcie dla funkcji wczesnego ostrzegania, które informuje użytkownika o potencjalnych problemach jeszcze przed ich wystąpieniem, co minimalizuje ryzyko awarii.</p> <p>50.1.4. Analiza historii zdarzeń: System diagnostyczny musi umożliwiać przeglądanie pełnej historii zdarzeń oraz błędów, co ułatwia analizę przyczyn awarii i planowanie działań naprawczych.</p> <p>51. Zaawansowane monitorowanie dysków twardych</p> <p>51.1. System musi oferować szczegółowe monitorowanie stanu dysków twardych z podziałem na:</p> <p>51.1.1. Alarmy dotyczące oprogramowania układowego dysku (firmware): Wykrywanie błędów związanych z oprogramowaniem układowym dysków oraz informowanie o konieczności aktualizacji firmware'u.</p> <p>51.1.2. Alarmy dotyczące konfiguracji dysków: Monitorowanie nieprawidłowej konfiguracji dysków, takich jak problemy z RAID, oraz informowanie o konieczności interwencji.</p> <p>51.1.3. Alarmy dotyczące usterek fizycznych: Wykrywanie błędów fizycznych dysków, takich jak problemy mechaniczne lub sektory uszkodzone, z możliwością precyzyjnego wskazania wadliwego dysku.</p> <p>52. Monitorowanie temperatury i zarządzanie termiczne</p> <p>52.1. System diagnostyczny musi zapewniać:</p> <p>52.1.1. Graficzną mapę temperatury: Wymagana jest funkcjonalność przeglądania rozkładu temperatury wewnątrz serwera w formie graficznego modelu 3D. Mapa temperatury musi umożliwiać szybkie lokalizowanie anomalii termicznych.</p> <p>52.1.2. Alerty dotyczące przekroczenia temperatur: Automatyczne powiadamianie o przekroczeniu dopuszczalnych wartości temperatury dla kluczowych komponentów, takich jak procesory, pamięć RAM czy zasilacze.</p> <p>52.1.3. Dynamiczne zarządzanie chłodzeniem: System musi wspierać dynamiczne dostosowywanie prędkości wentylatorów na podstawie aktualnych odczytów temperatury, co zapewnia optymalną pracę serwera i minimalizuje zużycie energii.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>53. Szyfrowane powiadomienia o błędach</p> <p>53.1. Wymagane jest wsparcie dla szyfrowanych powiadomień o niekrytycznych i niekorygowalnych błędach (UCE), które umożliwiają precyzyjną identyfikację wadliwego modułu pamięci lub dysku.</p> <p>53.2. System musi wspierać funkcję wysyłania powiadomień o błędach do administratora poprzez e-mail oraz protokoły zarządzania (np. SNMP, Redfish API).</p> <p>54. Integracja z modułem zarządzania</p> <p>54.1. System diagnostyczny musi być w pełni zintegrowany z modułem zarządzania iBMC, co umożliwia dostęp do danych diagnostycznych z poziomu interfejsu zarządzania.</p> <p>54.2. Wymagana jest możliwość przeglądania szczegółowych raportów diagnostycznych oraz uruchamiania testów diagnostycznych w czasie rzeczywistym z poziomu konsoli zarządzającej.</p>
System operacyjny (8szt.)	<p>55. Każda licencja musi być przeznaczona dla środowiska serwerowego obsługującego co najmniej 16 rdzeni procesorowych.</p> <p>56. Charakterystyka systemu operacyjnego:</p> <p>56.1. Zaawansowany system operacyjny serwerowy, wspierający wirtualizację i zarządzanie środowiskami chmurowymi.</p> <p>56.2. Możliwość instalacji na serwerach wielordzeniowych w architekturze x64.</p> <p>56.3. Obsługa środowisk klastrowych i wirtualnych.</p> <p>57. Funkcjonalności oprogramowania:</p> <p>57.1. Możliwość uruchomienia do 2 maszyn wirtualnych na każdą licencję obejmującą 16 rdzeni procesorowych.</p> <p>57.2. Obsługa zaawansowanych funkcji bezpieczeństwa, w tym szyfrowania i ochrony przed złośliwym oprogramowaniem.</p> <p>57.3. Integracja z usługami katalogowymi i zarządzanie użytkownikami w środowisku Active Directory.</p> <p>57.4. Obsługa klastrów wysokiej dostępności.</p> <p>58. Wymagania licencyjne:</p> <p>58.1. Licencje muszą być przypisane do serwerów fizycznych i obejmować co najmniej 16 rdzeni na serwer.</p> <p>58.2. Każda licencja pozwala na uruchomienie do 2 maszyn wirtualnych na danym serwerze.</p> <p>58.3. Licencje wieczyste (perpetual).</p> <p>58.4. Licencje w wersji detalicznej (retail).</p> <p>58.5. W razie potrzeby uruchomienia większej liczby maszyn wirtualnych, dostarczone licencje muszą umożliwiać dokupienie dodatkowych.</p> <p>59. Wymagania dotyczące dostawy i legalności oprogramowania</p> <p>59.1. Licencje muszą być dostarczone w formie elektronicznej (np. klucz aktywacyjny) lub w formie fizycznej (np. nośnik instalacyjny z kluczem).</p> <p>59.2. Licencje muszą pochodzić od autoryzowanego dystrybutora lub producenta.</p> <p>59.3. Dostawca zobowiązany jest do zapewnienia dokumentacji potwierdzającej legalność oprogramowania, w tym:</p> <p>59.3.1. Warunków licencyjnych.</p> <p>59.3.2. Dokumentu potwierdzającego zakup.</p>
Certyfikaty	<p>60. Oferowany serwer musi być certyfikowany dla następujących środowisk:</p> <p>60.1. VMware ESXi (wymagana certyfikacja VMware HCL).</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>60.2. Microsoft Windows Server (wymagana zgodność z HCL Microsoft).</p> <p>61. Producent oferowanego serwera musi posiadać certyfikaty jakości i bezpieczeństwa:</p> <p>61.1. ISO 9001 lub równoważny dla Systemów Zarządzania Jakością.</p> <p>61.2. ISO 14001 lub równoważny dla Systemów Zarządzania Środowiskowego.</p> <p>61.3. ISO 50 001 lub równoważny dla Systemów Zarządzania Energią.</p> <p>61.4. QC 080000 (System Zarządzania Procesami Produktów Niebezpiecznych).</p> <p>61.5. Deklaracja CE dla oferowanego modelu serwera.</p> <p>61.6. Certyfikat EPEAT na poziomie min. Bronze.</p>
Efektywność energetyczna	<p>62. Oferowane urządzenie musi udostępniać narzędzie, które zapewni możliwość bieżącej analizy poboru prądu.</p> <p>63. Serwer musi być przystosowany do pracy w temperaturze od 5 do 40 stopni Celsjusza co musi być kompatybilne z wytycznymi ASHRAE A1 do A3.</p> <p>64. Oferowane urządzenie musi być przystosowane do pracy w środowisku określonym normą ISO 14644-1. Informacja na ten temat musi znajdować się w oficjalnej dokumentacji dotyczącej oferowanego serwera.</p> <p>65. Zasilacze muszą posiadać certyfikat 80 Plus PSU Titanium, zapewniający sprawność energetyczną na poziomie co najmniej 96% przy obciążeniu 50%.</p>
Dokumentacja użytkownika	<p>66. Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera.</p>
Dodatkowe oprogramowanie zabezpieczające	<p>67. System chroniący przed zagrożeniami musi posiadać certyfikaty:</p> <p>67.1. OPSWAT (dla EDR na poziomie min. Platinum),</p> <p>67.2. AV Comperative Advance +</p> <p>67.3. AV-TEST (ochrona w 2023 na poziomie min.6)</p> <p>67.4. Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6</p> <p>68. Szyfrowanie danych:</p> <p>68.1. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.</p> <p>68.2. Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.</p> <p>69. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.</p> <p>70. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.</p> <p>71. Istnieje możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>72. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.</p> <p>73. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.</p> <p>74. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.</p> <p>75. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.</p> <p>76. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przez niezamierzonymi manipulacjami – ataki ransomware</p> <p>77. Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:</p> <p>77.1. Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli</p> <p>77.2. Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory</p> <p>77.3. Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux</p> <p>77.4. Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.</p> <p>77.5. Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich</p> <p>77.6. Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji</p> <p>78. Zarządzanie przez Chmurę:</p> <p>78.1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach</p> <p>78.2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury</p> <p>78.3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur</p> <p>78.4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii, aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy</p> <p>78.5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach</p> <p>78.6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń</p> <p>78.7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>79. Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.</p> <p>80. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.</p> <p>81. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer</p> <p>82. Oprogramowanie klienckie, zarządzane z poziomu serwera.</p> <p>83. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:</p> <p>83.1. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie</p> <p>83.2. funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD</p> <p>83.3. funkcje regulowania połączeń WiFi i Bluetooth</p> <p>83.4. funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe</p> <p>83.5. funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi</p> <p>83.6. funkcje blokowania dostępu dowolnemu urządzeniu</p> <p>83.7. możliwość tymczasowego dodania dostępu do urządzenia przez administratora</p> <p>83.8. zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu</p> <p>83.9. możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka</p> <p>83.10. możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora</p> <p>83.11. możliwość zarządzania urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry</p> <p>83.12. możliwość używania tylko zaufanych urządzeń sieciowych w tym urządzeń wskazanych na końcówkach klienckich</p> <p>83.13. funkcję wirtualnej klawiatury</p> <p>83.14. możliwość blokowania każdej aplikacji</p> <p>83.15. możliwość zablokowania aplikacji w oparciu o kategorie</p> <p>83.16. możliwość dodania własnych aplikacji do listy zablokowanych</p> <p>83.17. zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjną na serwerze</p> <p>83.18. dodawanie innych aplikacji</p> <p>83.19. dodawanie aplikacji w formie portable</p> <p>83.20. możliwość wyboru pojedynczej aplikacji w konkretnej wersji</p> <p>83.21. dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB</p> <p>83.22. kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>83.23. możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.</p> <p>83.24. możliwość zablokowania funkcji Printscreen</p> <p>83.25. funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSX</p> <p>83.26. funkcje monitorowania i kontroli przepływu poufnych informacji</p> <p>83.27. możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików</p> <p>83.28. możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj</p> <p>83.29. możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe</p> <p>83.30. ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe</p> <p>83.31. ochrona zawartości schowka systemu</p> <p>83.32. ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL</p> <p>83.33. możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych</p> <p>83.34. ochrona plików zamkniętych w archiwach</p> <p>84. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem</p> <p>84.1. możliwość tworzenia profilu DLP dla każdej polityki</p> <p>84.2. wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania</p> <p>84.3. ochrona przed wyciekiem plików poprzez programy typu p2p</p> <p>85. Monitorowanie zmian w plikach:</p> <p>85.1. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.</p> <p>85.2. Funkcje monitorowania określonych rodzajów plików.</p> <p>85.3. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.</p> <p>85.4. Generator raportów do funkcjonalności monitora zmian w plikach.</p> <p>85.5. możliwość śledzenia zmian we wszystkich plikach</p> <p>85.6. możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach</p> <p>85.7. możliwość definiowania własnych typów plików</p> <p>86. Optymalizacja systemu operacyjnego stacji klienckich:</p> <p>86.1. usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku</p> <p>86.2. optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem</p> <p>86.3. możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich</p> <p>86.4. instruktaż stanowiskowy pracowników Zamawiającego</p> <p>86.5. dokumentacja techniczna w języku polskim</p> <p>87. Wspierane platformy i systemy operacyjne:</p> <p>87.1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>87.2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)</p> <p>87.3. Mac OS X, Mac OS 10</p> <p>87.4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat</p> <p>88. Platforma do zarządzania dla Android i iOS:</p> <p>88.1. Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę</p> <p>88.2. Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.</p> <p>89. Zarządzanie użytkownikiem</p> <p>89.1. Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email</p> <p>89.2. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika</p> <p>89.3. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi</p> <p>89.4. Musi posiadać możliwość eksportu danych użytkownika</p> <p>90. Zarządzanie urządzeniem</p> <p>90.1. Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO</p> <p>90.2. Musi umożliwiać import listy urządzeń z pliku CSV</p> <p>90.3. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych</p> <p>90.4. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta</p> <p>90.5. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał</p> <p>90.6. Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres</p> <p>90.7. Musi zawierać podgląd aktualnie zainstalowanych aplikacji</p> <p>90.8. Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,</p> <p>90.9. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł</p> <p>90.10. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres</p> <p>91. Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:</p> <p>91.1. Wymagania dotyczące technologii:</p> <p>91.1.1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową</p> <p>91.1.2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>91.1.3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:</p> <p>91.1.3.1. Microsoft Internet Explorer</p> <p>91.1.3.2. Microsoft Edge</p> <p>91.1.3.3. Mozilla Firefox</p> <p>91.1.3.4. Google Chrome</p> <p>91.1.3.5. Safari</p> <p>91.2. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących</p> <p>91.3. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie</p> <p>91.4. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:</p> <p>91.4.1. Windows 2008 R2</p> <p>91.4.2. Windows 2012</p> <p>91.4.3. Windows 2012 R2</p> <p>91.4.4. Windows 2016</p> <p>91.5. Portal zarządzający musi umożliwiać:</p> <p>91.5.1. przegląd wybranych danych na podstawie konfigurowalnych widgetów</p> <p>91.5.2. zablokowania możliwości zmiany konfiguracji widgetów</p> <p>91.5.3. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.</p> <p>91.5.4. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności</p> <p>91.5.5. eksport wszystkich skanów podatności do pliku CSV</p> <p>91.6. Backup i przywracanie danych</p> <p>91.6.1. Deduplikacja danych,</p> <p>91.6.2. Backup przyrostowy i różnicowy,</p> <p>91.6.3. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,</p> <p>91.6.4. Backup danych lokalnych – plikowy oraz poczty Outlook,</p> <p>91.6.5. Backup otwartych plików (VSS),</p> <p>91.6.6. Filtr plików oraz folderów,</p> <p>91.6.7. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),</p> <p>91.6.8. Wyłączanie komputera po wykonaniu backupu,</p> <p>91.6.9. Przywracanie danych do wskazanej lokalizacji,</p> <p>91.6.10. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,</p> <p>91.6.11. Wyszukiwanie plików w repozytorium użytkownika,</p> <p>91.7. Ustawienia</p> <p>91.7.1. Automatyczne logowanie,</p> <p>91.7.2. Zapamiętywanie danych logowania,</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	<p>91.7.3. Automatyczne uruchamianie programu przy starcie systemu, 91.7.4. Ustawianie priorytetu dla procesu backupu, 91.7.5. Zmiana klucza szyfrującego, 91.7.6. Ustawienia przepustowości/zajętości pasma, 91.7.7. Konfiguracja wydajności procesu backupu, 91.8. Bezpieczeństwo 91.8.1. Zastępowanie nazwy pliku GUID-em, 91.8.2. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 91.8.3. Kompresja danych, 91.8.4. Transmisja po bezpiecznym protokole TLS, 91.8.5. Deklaracja klucza szyfrującego dane użytkownika, 91.8.6. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 91.8.7. Obliczanie sumy kontrolnej, 91.8.8. Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.</p> <p>92. WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.</p> <p>93. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 lub inny równoważny dla podmiotu serwisującego w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.</p>
Warunki gwarancji	<p>94. Zamawiający wymaga zapewnienia oficjalnego wsparcia Producenta w ramach oferowanej technologii na okres min. 2 lat w trybie NBD.</p> <p>95. Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online.</p> <p>96. Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez Producenta.</p> <p>97. Wymagane dołączenie do oferty oświadczenia potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>98. Usługi serwisowe obejmują:</p> <p>98.1. Diagnostowanie problemów sprzętowych i programowych.</p> <p>98.2. Aktualizacje firmware oraz dostęp do najnowszych wersji sterowników przez okres trwania wsparcia.</p> <p>98.3. Naprawy na miejscu w siedzibie zamawiającego.</p> <p>98.4. Czas reakcji serwisu do następnego dnia roboczego.</p>

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
	98.5. Naprawy muszą być przeprowadzone przez certyfikowany personel Producenta lub autoryzowanego partnera serwisowego posiadającego certyfikację ISO 9001, ISO 27001 lub inny równoważny

2. Serwer NAS – 3 szt.

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Obudowa	1. Typu rack o wysokości maksymalnie 1U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie.
Procesor	2. Jeden procesor osiągający wynik minimum 4000 punktów w teście PassMark.
Pamięć RAM	3. Minimum 8GB DDR4 ECC w konfiguracji 1 x 8GB. Możliwość rozbudowy pamięci RAM do minimum 16GB.
Ilość obsługiwanych dysków	4. Minimum 4 dyski o maksymalnej pojemności nie mniejszej niż 16TB każdy, po podłączeniu modułów rozszerzających minimum 8 dysków.
Interfejsy sieciowe	5. Minimum 4 porty 1GbE RJ-45. Wsparcie dla agregacji łączy.
Wskaźniki LED	6. Status, HDD 1-4, zasilanie, LAN 1-4
Obsługa RAID	7. Minimum RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
Funkcje RAID	8. Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
Szyfrowanie	9. Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	10. SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	<p>11. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.</p> <p>12. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.</p> <p>13. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby</p>

	klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.
Zarządzanie dyskami	14. SMART, sprawdzanie złych sektorów.
Język GUI	15. Polski
Gwarancja i serwis	16. Minimum 2 lata gwarancji.
Pobór mocy	17. Maksymalnie 70W w trybie pracy.
Certyfikaty	18. CE, FCC
System plików	19. Dyski wewnętrzne: BTRFS.
Szyfrowanie	20. Mechanizm szyfrowania sprzętowego (AES-NI)
Zasilacz	21. Pojedynczy zasilacz o mocy minimum 100W.
Chłodzenie	22. Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej.
Wdrożenie	<p>23. Przygotowanie do wdrożenia</p> <p>23.1. Analiza infrastruktury: Wykonawca przeprowadzi analizę istniejącej infrastruktury sieciowej oraz systemów IT, aby zapewnić kompatybilność serwera NAS z obecnym środowiskiem.</p> <p>23.2. Planowanie wdrożenia: Na podstawie wyników analizy zostanie opracowany szczegółowy plan wdrożenia, obejmujący harmonogram działań, wymagania sprzętowe i licencyjne oraz scenariusz konfiguracji serwera NAS.</p> <p>24. Instalacja i konfiguracja sprzętowa</p> <p>24.1. Montaż serwera NAS: Wykonawca zamontuje serwer NAS w szafie rackowej, wykorzystując szyny przesuwne dostarczone w zestawie. Montaż będzie zgodny ze standardami montażowymi rack 1U.</p> <p>24.2. Podłączenie dysków HDD: Zostaną zamontowane dyski zgodne z listą kompatybilności serwera NAS i wymaganiami Zamawiającego (np. 4 x 8 TB). Dyski będą prawidłowo zamocowane w zatokach dyskowych, a serwer zostanie uruchomiony w celu wykrycia i inicjalizacji dysków.</p> <p>24.3. Konfiguracja chłodzenia: Wykonawca skonfiguruje wentylatory serwera z możliwością regulacji prędkości obrotowej, co zapewni optymalne chłodzenie w zależności od obciążenia.</p> <p>25. Konfiguracja logiczna serwera NAS</p> <p>25.1. Utworzenie wolumenów RAID: W oparciu o wymagania Zamawiającego zostaną skonfigurowane wolumeny RAID (np. RAID 1, 5, 6 lub 10). Wolumeny będą zabezpieczone z użyciem dysków zapasowych typu hot spare oraz funkcji pozwalających na wymianę dysków na większe bez utraty danych.</p> <p>25.2. Ustawienia sieciowe: Serwer NAS zostanie podłączony do sieci z wykorzystaniem co najmniej 4 portów 1 GbE RJ-45, z możliwością agregacji łączy w celu zapewnienia wyższej przepustowości i redundancji.</p> <p>25.3. Konfiguracja protokołów i usług sieciowych: Wykonawca skonfiguruje dostęp do serwera NAS za pośrednictwem protokołów SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP oraz usługi, takie jak serwer VPN, serwer</p>

	<p>pocztowy, serwer plików, serwer WWW, DDNS, LDAP, replikacja zdalna oraz funkcje szyfrowania danych.</p> <p>26. Zarządzanie i monitorowanie serwera</p> <p>26.1. Konfiguracja funkcji monitorowania: Aktywacja funkcji SMART i sprawdzania złych sektorów, które umożliwią bieżące monitorowanie stanu dysków twardych.</p> <p>26.2. Konfiguracja wskaźników LED: Ustawienie wskaźników LED dla monitorowania statusu serwera, dysków HDD, zasilania oraz sieci LAN, co zapewni administratorowi szybką diagnozę stanu urządzenia.</p> <p>26.3. Zarządzanie kopiami zapasowymi: Konfiguracja backupów typu bare-metal komputerów lokalnych, harmonogramu zdalnych kopii zapasowych, opcji przyrostowych kopii oraz deduplikacji danych.</p> <p>27. Testowanie i optymalizacja</p> <p>27.1. Testy funkcjonalności: Wykonawca przeprowadzi testy operacyjne, aby zweryfikować poprawność konfiguracji RAID, działanie połączeń sieciowych, funkcje zabezpieczeń oraz integrację z infrastrukturą sieciową i usługami Zamawiającego.</p> <p>27.2. Optymalizacja wydajności: Po testach wykonawca dokona optymalizacji ustawień, aby dostosować serwer NAS do specyficznych wymagań środowiska pracy, w tym ustawień RAID, polityk dostępu, protokołów oraz mechanizmów szyfrowania.</p>
--	---

3. Dyski twarde do macierzy dyskowej (serwera NAS) – 3 kpl.

PARAMETR	CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Ogólne	<p>1. 4 dyski twarde HDD o pojemności 8 TB każdy, przeznaczone do współpracy z oferowanymi serwerami NAS. Dostarczone dyski muszą być zgodne z listą kompatybilności systemu oraz spełniać minimalne wymagania techniczne określone poniżej.</p>
Wymagania techniczne	<p>2. Pojemność: 8 TB każdy.</p> <p>3. Interfejs: SATA 6 Gb/s.</p> <p>4. Prędkość obrotowa: minimum 7200 RPM, zapewniająca szybki dostęp do danych oraz optymalną wydajność.</p> <p>5. Pamięć cache: minimum 250 MB, co umożliwia sprawną obsługę operacji odczytu i zapisu.</p> <p>6. Współczynnik niezawodności MTBF (Mean Time Between Failures): minimum 1 milion godzin, co gwarantuje wysoką trwałość i niezawodność w środowisku pracy 24/7.</p>
Gwarancja	<p>7. minimum 24 miesiące od daty dostawy, obejmująca wsparcie techniczne i ewentualną wymianę w razie awarii.</p>

4 Wymagania, termin wykonania oraz nazwy i kody dotyczące przedmiotu zamówienia określone we Wspólnym Słowniku Zamówień Publicznych

1. Jeżeli dokumentacja zamówienia wskazywałyby znaki towarowe, patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę (Zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób) oraz mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów Zamawiający, zgodnie z art. 99 Pzp, dopuszcza składanie produktów równoważnych. Wszelkie produkty pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać oferowane produkty, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dotyczący minimalnych wymagań parametrów jakościowych, Zamawiający rozumie wymagania produktów zawarte m.in. w ogólnie dostępnych źródłach, katalogach, na stronach internetowych producentów. Operowanie przykładowymi nazwami, ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami produktów ma wyłącznie charakter przykładowy. Zamawiający wskazując oznaczenie konkretnego produktu, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych.
 2. Główny kod CPV:
48820000-2 – Serwery.
 - Dodatkowe kody CPV:
32420000-3 – Urządzenia sieciowe,
72000000-5 – Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia,
72263000-6 – Usługi wdrażania oprogramowania.
 3. Termin wykonania przedmiotu zamówienia: **do 60 dni** kalendarzowych liczonych od daty zawarcia umowy.
 4. Wymagania powinny być potwierdzone dokumentami dołączonymi do oferty:

Nazwa	Wymagane dokumenty – załączniki oferty
1. Serwer kopii zapasowej – klaster wysokiej dostępności	<p>W odniesieniu do serwera:</p> <ol style="list-style-type: none"> 1.1. Certyfikat ISO 9001 lub równoważny dla Systemów Zarządzania Jakością. 1.2. Certyfikat ISO 27001 lub równoważny dla Systemów Bezpieczeństwa Informacji. 1.3. Certyfikat ISO 14001 lub równoważny dla Systemów Zarządzania Środowiskowego. 1.4. Certyfikat ISO 50001 lub równoważny dla Systemów Zarządzania Energią. 1.5. Certyfikat QC 080000 lub równoważny dla Systemów Zarządzania Procesami Produktów Niebezpiecznych. 1.6. Deklaracja CE dla oferowanego modelu serwera. 1.7. Certyfikat EPEAT na poziomie min. Bronze. 1.8. Dokumenty potwierdzające, że serwis sprzętu będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta wraz z certyfikatem: ISO 9001 (o którym mowa w ppkt 1.1.) oraz 27001 (o którym mowa w ppkt 1.2.) lub innymi równoważnymi dla podmiotu serwisującego sprzęt. <p>2. W odniesieniu do zasilaczy:</p> <ol style="list-style-type: none"> 2.1. Certyfikat Titanium zgodnie z programem certyfikacji 80 Plus PSU lub inny równoważny.

	3. W odniesieniu do oprogramowania zabezpieczającego: 1.1. 3.1. Certyfikat ISO 9001 oraz 27001 lub inny równoważny dla podmiotu serwisującego sprzęt w zakresie świadczenia usług wsparcia technicznego oraz usług zwianych z cyberbezpieczeństwem dla podmiotu serwisującego sprzęt.
2. Serwer NAS	Brak wymaganych dokumentów.
3. Dyski twarde do macierzy dyskowej (serwera NAS)	Brak wymaganych dokumentów.