Załącznik nr 1B

OPIS PRZEDMIOTU ZAMÓWIENIA

Projekt „Cyfrowy Powiat" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020.

SPIS TREŚCI

Wstęp

Niniejszy dokument określa minimalne wymagania dla przedmiotu zamówienia dotyczącego realizacji projektu pn.: „Cyfrowy Powiat" realizowanego przez Powiat Lubański.

Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowy Powiat" umowa o powierzenie grantu o numerze 5594/P/2022.

Serwer wraz licencjami na systemy – 1 szt.

Nazwa	Minimalne wymagania dla sprzętu
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3,5” • Możliwość wyposażenia w panel LCD
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym • Płyta główna powinna obsługiwać rozbudowę do min. 128GB pamięci • Na płycie głównej powinny znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor minimum 6-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 51.4 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej.
Pamięć RAM	• Minimum 1x16GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	• min. 3 porty USB w tym 1 port USB 3.0 z tyłu obudowy, • 1 port VGA na tylnym panelu, • 1 port RS232
Gniazda PCI	Min. 3 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
Dyski twarde	• Zainstalowane 4 dyski SATA, 7200RPM, o pojemności minimalnej 8TB, 6Gbps, 3,5”, Hot-Plug. • Gwarancja na dyski 36 miesięcy. • W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.
Wentylatory	Wentylatory redundantne
Zasilacz	Redundantny, Moc maks. 600W.
System operacyjny	Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. Wykonawca odpowiada za sprawne i wydajne działanie systemu operacyjnego na dostarczonym sprzęcie serwerowym. Poniższy opis należy traktować jako zbiór wymagań minimalnych, ponieważ Wykonawca musi zapewnić odpowiednie parametry i spełnić wszystkie wymagania licencyjne oferowanego systemu operacyjnego, niezbędne do poprawnego uruchomienia rozwiązania. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć

	Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów,

	VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Dodatkowe oprogramowanie	VMware vSphere 8 Essentials Kit for 3 hosts (Max 2 CPU per host, 32 cores/CPU) – licencja z rocznym wsparciem
Opis systemu operacyjnego i dodatkowego oprogramowania	1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 3 dwuprocesorowych fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM. 6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.

	12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS. 13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 14. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 16. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 17. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 18. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). 19. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM. 20. Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora. 21. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 22. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 23. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej. 24. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5. 25. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne. 26. Rozwiązanie musi zawierać wsparcie dla TPM 2.0 oraz wirtualnego TPM.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

	• możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej • Przesyłanie danych telemetrycznych w czasie rzeczywistym • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze • Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

	• Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Certyfikat ISO 9001 dla producenta sprzętu • Certyfikat ISO 14001 dla producenta sprzętu • Deklaracja zgodności CE • Certyfikat ISO 50001 • Potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Gwarancji producenta: minimum 36 miesięcy • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.

	• W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • Serwis sprzętu musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

Urządzenie typu NAS – 1 szt.

Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark co najmniej 4500 punktów
Obudowa	Typu rack o wysokości max 2U i wymiarach maksymalnych 90 mm x 490 mm x 410 mm (wysokość x szerokość x głębokość) wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie.
Pamięć RAM	Minimum 32 GB DDR4 ECC. Kompatybilność pamięci RAM musi być oficjalnie potwierdzona na stronie producenta serwera NAS.
Ilość obsługiwanych dysków	Minimum 8 dysków o maksymalnej pojemności 18TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków.
Zainstalowane dyski	4 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanej macierzy oraz charakteryzujących się następującymi parametrami: - interfejs: SATA 6Gb, - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256 MB, - gwarancja: minimum 36 miesięcy, - MTBF: minimum 1 milion.
Interfejsy sieciowe	Minimum 2 porty 1GbE RJ-45, Minimum 2 porty 10GbE SFP+, Wsparcie dla Link Agregation, Funkcja Wake on LAN/WAN
Porty	Minimum 2 porty USB 3.2 Gen 1. 1 gniazdo rozszerzenia eSATA Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń PCIe x8
Wskaźniki LED	Status, HDD 1-8, zasilanie, LAN 1-4
Obsługa RAID	Basic, JBOD, RAID 0, 1, 5, 6, 10, SHR. Obsługa dysków typu hot spare.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV, WebDAV, Telnet, SSH, AFP, VPN (PPTP, OpenVPN™, L2TP)
Usługi	1. Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, 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. 2. Możliwość utworzenia klastra wysokiej dostępności (High Availablity) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.
Obsługa migawek	Minimalna liczba migawek folderu współdzielonego: 1000 Minimalna liczba migawek w całym systemie operacyjnym: 65000
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów
Język GUI	Polski
Gwarancja i serwis	Minimum 3 lata gwarancji NBD na serwer – dostawa urządzenia zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej.
Waga	Maksymalnie 12 kg
Pobór mocy	Maksymalnie 65W w trybie pracy. Maksymalnie 35W w trybie hibernacja dysków.
Certyfikaty	FCC, CE
System plików	Dyski wewnętrzne Btrfs lub EXT4. Dyski zewnętrzne Btrfs, FAT32, NTFS, EXT3, EXT4, HFS+, exFAT*(z dodatkową licencją) Zarządzanie pamięcią masową
Szyfrowanie	Mechanizm szyfrowania sprzętowego (AES-NI)
Liczba wolumenów	Minimum 64
Liczba iSCSI Targetów	Minimum 128
Liczba iSCSI LUN	Minimum 256
Rozmiar pojedynczego wolumenu:	Minimum 108 TB
Liczba kont użytkowników	Minimum 2000
Liczba grup	Minimum 250
Liczba folderów udostępnionych	Minimum 500
Ilość jednoczesnych połączeń	Minimum 1000 dla CIFS/AFP/NFS/FTP/WebDAV
Zasilacz	Redundantny zasilacz o mocy maksymalnie 350W
Chłodzenie	Minimum 2 wentylatory o rozmiarze nie większym niż 80 mm x 80 mm
Wymagania dodatkowe	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) Obsługa min. VMware vSphere, Microsoft Hyper-V, Citrix, OpenStack Usługa katalogowa: Łączy się z serwerami Windows AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File Station przy użyciu istniejących poświadczeń. Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) Obsługiwane systemy klienckie: min. Windows7 i nowsze, macOS 10.12 i nowsze Obsługiwane przeglądarki Chrome, Firefox, Edge, Internet Explorer 10 i nowsze, Safari 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android 6.0 i nowsze) na tabletach Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Oprogramowanie do tworzenia kopii zapasowych musi umożliwiać wykonywanie testów

	tworzonych kopii bez całościowego przywracania zabezpieczonego środowiska, z możliwością generowania potwierdzenia poprawności lub niepoprawności stworzonej kopii. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.
Gwarancja	Gwarancja z czasem reakcji na następny dzień roboczy (NBD). Wykonawca udzieli gwarancji: • Minimum 36 miesięcy na urządzenie główne • Minimum 12 miesięcy na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack.

Przełącznik sieciowy (switch) – 2 szt.

Nazwa	Minimalne wymagania dla sprzętu
Typ	Sieciowe urządzenie przełączające wielowarstwowe: L2/L2+ z funkcją PoE.
Obudowa	• Obudowa Rack o wysokości max 1U, • Możliwość montażu w szafie teledacyjnej RACK (niezbędne dostarczenie wyposażenia do zamontowania urządzenia w szafie tj. uchwyty, zaczepy, śruby itp.), • Wbudowany zasilacz: 100-240V AC, 50/60Hz • Dołączony kabel zasilający zakończony wtykiem standardowym (wykorzystywanym w Polsce), • Maksymalne zużycie energii: 180W (220 V/50 Hz) (przy zasilaniu z mocą 150 W)
Interfejsy	• 16 portów 10/100/1000 Mb/s RJ45 PoE+ (Auto-negocjacja/Auto MDI/MDIX) • Zgodność ze standardami 802.3af (PSE) do 15.4W • Zgodność ze standardami 802.3at (PSE) do 30W • Moc zasilania PoE min. 150W • Dodatkowo co najmniej 2 Gigabitowe sloty SFP Obsługiwane okablowanie min.: • 10BASE-T: Kabel UTP kat. 3, 4 lub 5 (do 100m), • 100BASE-TX/1000Base-T: Kabel UTP kat. 5, 5e, lub wyższej (do 100m), • 1000BASE-X: MMF, SMF
Wydajność	• Wydajność przełączania min. 36 Gbit/s, • Szybkość przełączania min. 26 Mpps, • Tablica adresów MAC min. 8K, • Bufor pakietów min. 4 Mbit, • Ramki jumbo min. 9KB
Zarządzanie	• Przy pomocy dostarczonego systemu zarządzania/aplikacji producenta przełącznika, • Przy pomocy przeglądarki web (również HTTPS z szyfrowaniem min. SSLv3/TLS 1.2), • Przy pomocy linii komend (CLI) (również z szyfrowaniem min. SSHv1/SSHv2), • Oparte na rozwiązaniu chmurowym, • Zarzadzanie zcentralizowane.

Funkcje panelu zarządzania	• SNMP v1/v2c/v3, • SNMP Trap/Inform, • RMON (grupy 1, 2, 3, 9), • Szablon SDM, • Klient DHCP/BOOTP, • Dual Image, Dual Configuration, • Monitorowanie zużycia procesora, • Diagnostyka kabli, • EEE, • SNTP, • Logi systemu
Funkcje oprogramowania	**Funkcja Quality of Service:** • Obsługa priorytetowania 802.1p CoS/DSCP • 8 kolejek priorytetowania • Tryb harmonogramu priorytetowania: - SP (Strict Priority) - WRR (Weighted Round Robin) • Konfiguracja wagi kolejek • Kontrola przepustowości - Ograniczanie prędkości transferu w oparciu o port/przepływ danych • Płynniejsze działanie • Storm Control - Wiele trybów kontroli (kb/s/wskaźnik) - Kontrola transmisji Broadcast/Multicast/Unknown-Unicast **Funkcje L2 i L2+** • 16 Interfejsów IP - Obsługa interfejsu IPv4/IPv6 • Routing statyczny - 32 trasy statyczne IPv4/IPv6 • Serwer DHCP • DHCP Relay - DHCP Interface Relay - DHCP VLAN Relay • DHCP L2 Relay • Wpisy statyczne ARP • Proxy ARP • Gratuitous ARP • Agregacja łączy - Statyczna agregacja łączy - Do 8 grup agregacji i do 8 portów na grupę - LACP 802.3ad • Protokół Spanning Tree (STP) - STP 802.1D - RSTP 802.1w - MSTP 802.1s - Zabezpieczenia STP: ochrona TC, filtrowanie/ochrona poprzez pakiety BPDU, ochrona Root • Wykrywanie pętli zwrotnych • Kontrola przepływu - Kontrola przepływu 802.3x • Mirroring - Port Mirroring

	- Mirroring procesora - Przesył One-to-One - Przesył Many-to-One - W oparciu o przepływ - Port wejścia/wyjścia / obydwa porty • Device Link Detect Protocol (DLDP) • 802.1ab LLDP/ LLDP-MED **Sieci VLAN:** • Grupy VLAN - Maks. 4K grup VLAN • Tagowanie 802.1Q VLAN • Adres MAC VLAN: 12 wpisów • Protokół VLAN • GVRP • Głosowa sieć VLAN **Listy kontroli dostępu:** • Obsługa do 230 wpisów • Przedziały czasowe - Kwant czasu - Przedział czasowy w tygodniu - Uniwersalny przedział czasowy - Okres wakacji • Lista kontroli dostępu (ACL) oparta o czas • Adres MAC ACL - Źródłowy adres MAC - Docelowy adres MAC - ID sieci VLAN - User Priority - Ethertype • Adres IP ACL - Źródłowy adres IP - Docelowy adres IP - Protokół IP - Flaga TCP - Port źródłowy TCP/UDP - Port docelowy TCP/UDP - DSCP/TOS adresu IP • ACL IPv6 • Łączona ACL • Działania reguł - Zezwalaj/Odrzuć • Polityka kontroli dostępu - Mirror - Limit prędkości - Redirect - QoS Remark • Reguła wiązania ACL - Wiązanie portów - Wiązanie VLAN • Działania dla przepływów - Mirror (do obsługiwanego interfejsu)

	- Redirect (do obsługiwanego interfejsu) - Limit prędkości - QoS Remark **Bezpieczeństwo transmisji:** • AAA • Uwierzytelnianie 802.1X - Uwierzytelnianie w oparciu o port - Uwierzytelnianie w oparciu o adres MAC (Host) - Dostępne metody uwierzytelniania: PAP/EAP-MD5 - MAB - Sieć VLAN dla gości - Uwierzytelnianie i autoryzowanie poprzez Radius • Wiązanie adresów IP/IPv6 i MAC - 512 możliwych wpisów - DHCP Snooping - DHCPv6 Snooping - Inspekcja ARP - Wykrywanie ataków ND • Ochrona źródłowego adresu IP - 253 możliwych wpisów - Źródłowy adres IP + źródłowy adres MAC • Ochrona źródłowego adresu IPv6 - 183 możliwych wpisów - Źródłowy adres IPv6 + źródłowy adres MAC • Ochrona przed atakami DoS • Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację - Do 64 adresów MAC na port • Storm Control Broadcast/Multicast/Unicast - tryb kontroli (kb/s/wskaźnik) • Izolacja portów • Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2 • Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2 • Kontrola dostępu w oparciu o IP/port/MAC **IPv6:** • Routing statyczny i ACL IPv6 • IPv6 Dual IPv4/IPv6 • Interfejs IPv6 • Multicast Listener Discovery (MLD) Snooping • Funkcja neighbor discovery (ND) IPv6 • Path maximum transmission unit (MTU) discovery • ICMP v6 • TCP v6/UDP v6 • Zastosowania protokołu IPv6: - Klient DHCPv6 Client - Ping6 - Tracert6 - Telnet (v6) - SNMP IPv6 - SSH IPv6 - SSL IPv6 - Http/Https

	- TFTP IPv6 **Funkcje zaawansowane:** • Automatyczne wykrywanie urządzeń • Konfiguracja Batch • Aktualizacja oprogramowania Batch • Inteligentne monitorowanie sieci • Ostrzeżenia o nietypowych zdarzeniach • Ujednolicona konfiguracja • Harmonogram restartów **MIBs:** • MIB II (RFC1213) • Bridge MIB (RFC1493) • P/Q-Bridge MIB (RFC2674) • Radius Accounting Client MIB (RFC2620) • Radius Authentication Client MIB (RFC2618) • Zdalny Ping, Traceroute MIB (RFC2925) • Wsparcie dla prywatnego TP-Link MIB • RMON MIB(RFC1757, rmon 1,2,3,9)
Standardy i protokoły	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3az, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p, IEEE 802.1x
Gwarancja	Gwarancja producenta: min. 36 miesięcy
Certyfikaty	CE, FCC, RoHS

Wymagania dodatkowe

W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do dostawy przedmiotu zamówienia do wyznaczonego przez Zamawiającego pomieszczenia na terenie urzędu.

Wykonawca zobowiązany jest do ustalenia terminów dostaw z Zamawiającym, we wskazanym przez niego miejscu, z uwzględnieniem charakteru pracy Urzędu. Zamawiający dokona weryfikacji zgodności dostarczonego przedmiotu zamówienia w ciągu 3 dni roboczych od daty dostawy.