Załącznik nr 1 do Zaproszenia do złożenia propozycji cenowej w zakresie dostawy 2 serwerów wraz z oprogramowaniem

**Obudowa**

● Typu RACK, wysokość nie więcej niż 1U;

● Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz opcjonalnym z ramieniem porządkującym kable;

● Możliwość zainstalowania 10 dysków twardych hot plug 2,5” SATA/SAS;

● Możliwość rozbudowy o panel diagnostyczny z wyświetlaczem LCD umożliwiającym detekcję usterek umożliwiający wyświetlenie następujących informacji:

● aktywne ostrzeżenia;

● status serwera;

● typ oraz model serwera, numer seryjny;

● wersje oprogramowania UEFI oraz modułu zarządzania;

● informacje nt modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS;

● dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii;

● aktywne sesje połączeniowe do interfejsu zarządzania;

● Zainstalowane 2 szt. dysków SSD SATA M.2 480GB, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID;

**Płyta główna**

● Dwuprocesorowa;

● Wyprodukowana i zaprojektowana przez producenta serwera;

● Możliwość instalacji procesorów 60-rdzeniowych;

● Moduł TPM 2.0;

● 2 złącza PCI Express x16 generacji 4;

● Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;

● 32 gniazda pamięci RAM;

● Obsługa 8 TB pamięci operacyjnej RAM DDR5;

● Wsparcie dla technologii:

● Bounded Fault;

● SDDC;

● ECC;

● Memory Mirroring;

● ADDDC;

● Wewnętrzny slot na kartę Micro SD

**Procesory**

● Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,0 GHz, architektura x86\_64;

● osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 389 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla oferowanego serwera.

**Pamięć RAM**

● 256GB pamięci RAM;

● DDR5 Registered 5600MT/s;

● Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;

**Kontrolery LAN**

● Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):

● 4x 10Gbit Base-T;

● Możliwość uzyskania 2 interfejsów 100Gbit QSFP56 bez konieczności instalacji kart w slotach PCIe;

● 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;

● Interfejsy LAN zainstalowane w slotach PCI-e:

● 4x 10Gbit Base-T.

**Kontrolery I/O**

● Możliwość rozbudowy o Kontroler SAS RAID dla dysków wewnętrznych obsługujący następujące poziomy RAID: 0,1,10,5,50,6,60 posiadający 2GB pamięci cache zabezpieczonej przed utratą danych na wypadek awarii zasilania (tzw. podtrzymanie pamięci cache), obsługa globalnych dysków Hot-Spare oraz rozszerzanie pojemności logicznych przestrzeni on-line;

**Porty**

● Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera;

● 3 porty USB dostępne z tyłu serwera w tym dwa w wersji USB 3.2;

● 2 porty USB na panelu przednim w tym jeden w wersji USB 3.2;

● Jeden z frontowych portów USB musi posiadać możliwość zarządzania serwerem;

● Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;

● Opcjonalny port serial;

● Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

**Zasilanie, chłodzenie**

● Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1100W;

● Redundantne dwuwirnikowe wentylatory hotplug o prędkości obrotowej 25 000 obr./min. dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni celsjusza;

**Bezpieczeństwo**

● Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;

● Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;

● Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem;

● Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;

● Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;

● Możliwość wyłączenia w BIOS funkcji przycisku zasilania;

● Możliwość ustawienia hasła włączania serwera;

● Możliwość ustawienia hasła administratora;

● Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

**Zarządzanie**

● Wymaga się aby serwer posiadał diody sygnalizującę awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.

● Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser’ów PCIe, backplane’ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;

● Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.

● Funkcjonalność kontrolera zdalnego zarządzania:

● Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna

● Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarzadzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja

● Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.

● Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.

● Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3

● Update systemowego firmware

● Monitoring i możliwość ograniczenia poboru prądu

● Zdalne włączanie/wyłączanie/restart

● Zapis video zdalnych sesji

● Podmontowanie lokalnych mediów z wykorzystaniem Java client

● Przekierowanie konsoli szeregowej przez IPMI

● Zrzut ekranu w momencie zawieszenia systemu

● Możliwość przejęcia zdalnego ekranu

● Możliwość zdalnej instalacji systemu operacyjnego

● Alerty Syslog

● Przekierowanie konsoli szeregowej przez SSH

● Wsparcie dla dynamic DNS

● Wyświetlanie danych aktualnych I historycznych dla zużycia energii oraz temperatury serwera

● Wirtualna konsola z dostępem do myszy, klawiatury;

● Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy AciveX (musi działać w oparciu o HTML5)

● Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS

● Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę

● wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API

● Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.

● Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.

● Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot’u.

● Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.

● Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.

● Możliwość rozszerzenia funkcjonalności zarządzania i monitoringu serwerów o oprogramowanie producenta serwera spełniające poniższe wymagania:

● Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych

● Integracja z Active Directory

● Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym

● Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP

● Szczegółowy opis wykrytych systemów oraz ich komponentów

● Możliwość eksportu danych min do formatu CSV

● Grupowanie urządzeń w oparciu o kryteria użytkownika

● Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK

● Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS

● Szybki podgląd stanu środowiska

● Podsumowanie stanu dla każdego urządzenia

● Szczegółowy status urządzenia/elementu/komponentu

● Filtry raportów umożliwiające podgląd najważniejszych zdarzeń

● Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych

● Możliwość przejęcia zdalnego pulpitu

● Możliwość zamontowania wirtualnego napędu

● Kreator umożliwiający dostosowanie akcji dla wybranych alertów

● Przesyłanie alertów „as-is” do innych konsol firm trzecich

● Możliwość definiowania ról administratorów

● Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

● Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta

● Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)

● Automatyczna polityka aktualizacji „Najnowsze dostępne”

● Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym

● Możliwość automatycznego generowania i zgłaszania incydentów awari bezpośrednio do centrum serwisowego producenta serwerów

● Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta

● Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.

● Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

● Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI

● Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach

● Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

● Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:

● wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze Vmware do zdefiniowanej polityki poziomu mikrokodów

● wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji

● z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)

● inwentaryzacja komponentów w serwerze i ich mikrokodów

● historia min 24h poboru mocy i temperatury serwera

● zbieranie danych diagnostycznych serwera do paczki

● Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:

● wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze do zdefiniowanej polityki poziomu mikrokodów

● z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)

● aktualizacja sterowników systemowych Windows

● inwentaryzacja komponentów w serwerze i ich mikrokodów

● historia min 24h poboru mocy i temperatury serwera

● zbieranie danych diagnostycznych serwera do paczki

● Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

**Certyfikowane systemy operacyjne**

● Microsoft Windows Server 2025, 2022, 2019;

● VMWare ESXi 8.0, 7.0;

● Suse Linux Enterprise Server 15;

● Red Hat Enterprise Linux 9.x, 8.x;

● Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS,

● Microsoft Windows 11

● Oracle Linux 8.x, 9.x;

● Xen Server 8, Xen Hypervisor 8.2

**Licencja SSO**

Licencja na serwerowy system operacyjny w najnowszej dostępnej komercyjnie wersji musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie 4 instancji wirtualnych tego serwerowego systemu operacyjnego na tym serwerze. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.

2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

4) 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.

5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18) Mechanizmy logowania w oparciu o:

a) Login i hasło,

b) Karty z certyfikatami (smartcard),

c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b) 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:

i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.

d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

i. Dystrybucję certyfikatów poprzez http

ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.

g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i) Serwis udostępniania stron WWW.

j) Wsparcie dla protokołu IP w wersji 6 (IPv6),

k) Wsparcie dla algorytmów Suite B (RFC 4869),

l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 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:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

**Gwarancja**

● 3 lata gwarancji producenta serwera w trybie on-site z czasem reakcji następnego dnia roboczego. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;

● Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;

● Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera w 24h od zgłoszenia usterki (podać koszt na dzień składania oferty).

**Dokumentacja, inne**

● Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;

● Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

● Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;

● Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.