*Nr postępowania PFiZP 271.2.2023*

Załącznik nr 6 do SWZ

**Szczegółowy Opis Przedmiotu Zamówienia**

**WYMAGANIA DLA WYKONAWCY (DOTYCZY WSZYSTKICH ZADAŃ):**

1. Wykonawca oświadcza, że do wykonania przedmiotu umowy posiada niezbędne uprawnienia, wiedzę i doświadczenie, oraz dysponuje potencjałem ekonomicznym i technicznym, odpowiednim stanem zatrudnienia wykwalifikowanych pracowników lub zleceniobiorców lub innych osób współpracujących oraz że przedmiot umowy wykona zgodnie z obowiązującymi przepisami i normami.
2. Oferowane przez Wykonawcę sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, pełnowartościowe, wolne od wad prawnych i fizycznych oraz nie mogą naruszać praw majątkowych osób trzecich.
3. Wykonawca zobowiązuje się udzielić bezterminowych licencji na dostarczone oprogramowanie w taki sposób, aby Zamawiający był uprawniony do:
4. korzystania z wszystkich funkcjonalności odsprzedawanego oprogramowania w dowolny sposób.
5. instalowania odsprzedanego oprogramowania na sprzęcie Zamawiającego.
6. wykonywania kopii zapasowych dostarczanych przez Wykonawcę nośników oraz zainstalowanych odsprzedanych oprogramowań.
7. aktualizowania oprogramowania, na które udzielono licencji.
8. instalowania wszelkich poprawek opublikowanych na stronach wytwórcy oprogramowania.
9. Dostawa przedmiotu umowy oraz serwis powinny być wyznaczone na dzień roboczy tj. od poniedziałku do piątku w godzinach pracy Zamawiającego   
   tj. od 7:30 do 14.00.
10. Zawarta poniżej specyfikacja urządzeń określa minimalne parametry jakie powinien spełniać oferowany sprzęt.

**Zadanie nr 1- Dostawa Stacji roboczej All in One – 15 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Typ | Komputer stacjonarny typu All in One, komputer fabrycznie wbudowany w obudowę monitora |
|  | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
|  | Procesor | Zaoferowany procesor musi uzyskiwać w teście Passmark CPU Mark wynik min.: **3900** punktów - wynik zaproponowanego procesora musi znajdować się na stronie <https://www.cpubenchmark.net/cpu_list.php> **z dnia składania ofert (wynik załączyć do oferty)**  W przypadku użycia przez oferenta testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego. |
|  | Pamięć operacyjna RAM | 1 x 8GB,min. jeden slot wolny na dalszą rozbudowę,możliwość rozbudowy do min 16GB |
|  | Parametry pamieci masowej | Min. 512 GB SSD,możliwość rozbudowy o drugi dysk |
|  | Karta graficzna | Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12, osiągająca w teście Average G3D Mark wynik na poziomie min.: **800** punktów - wynik zaproponowanej grafiki musi znajdować się na stronie <https://www.videocardbenchmark.net/mid_range_gpus.html> **z dnia składania ofert (wynik załączyć do oferty)** |
|  | Wyposażenie multimedialne | Karta dźwiękowa, wbudowane 2 głośniki (stereo)  Wbudowana w obudowę matrycy cyfrowa kamera, chowana w obudowie  Wbudowany mikrofon |
|  | Matryca | Min. 21 cali, Rozdzielczość 1920 x 1080 FHD, Matrca IPS |
|  | Zgodność z systemami operacyjnymi i standardami | Zgodność z 64-bitową wersją systemu operacyjnego Microsoft Windows 10 Professional PL, zainstalowany system operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft |
|  | Porty/złącza | Wbudowane porty 1 x HDMI, 2 x USB 2.0, 2 x USB 3.2 typ A, 1 x RJ45,  1 x audio jack |
|  | Certyfikaty i standardy | Komputer musi być wyprodukowany zgodnie z normą ISO9001 i ISO 5001 –  certyfikaty dla producenta sprzętu **załączyć na wezwanie zamawiającego;**  Certyfikat ISO 50001 dla producenta sprzętu **- załączyć na wezwanie**  **zamawiającego;**  Oświadczenie producenta sprzętu, że oferowany sprzęt pochodzi  z autoryzowanego kanału sprzedaży na rynek UE **– załączyć na wezwanie**  **zamawiającego** |
|  | BIOS | BIOS zgodny z UEFI.  Wymagane informacje z poziomu BIOS na potrzeby inwentaryzacji:  wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach), procesor (typ, nazwa, prędkość, cache L2 i L3), pojemności zainstalowanych dysków twardych, MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio.  Informacje muszą być dostępne w menu BIOS bez stosowania dodatkowego  oprogramowania jak i wbudowanego systemu diagnostycznego.  Możliwość, ustawienia hasła na poziomie:  - administratora [hasło nadrzędne]  - użytkownika/systemowego - hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywanie zmian ustawień BIOS, rozruch systemu operacyjnego - hasło  blokuje start systemu operacyjnego.  Funkcja blokowania/odblokowania BOOTowania stacji roboczej z zewnętrznych urządzeń.  Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA, kontrolera  audio, układu TPM, wbudowanej kamery i czytnika kart multimedialnych,  czujnika otwarcia obudowy, ustawienia go w tryb cichy  Możliwość przypisania w BIOS numeru nadawanego przez Administratora  oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym.  Możliwość zdefiniowania automatycznego uruchamiania komputera codziennie  lub w wybrane dni tygodnia,  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu  komputer nie wykrywa urządzeń bootujących typu USB, natomiast po  uruchomieniu systemu operacyjnego porty USB są aktywne.  Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej  kombinacja.  BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku. |
|  | Wymagania dodatkowe | W zestawie klawiatura QWERTY USB w układzie polski programisty z wydzieloną klawiaturą numeryczną, mysz optyczna z 2 przyciskami oraz rolką |

**Zadanie nr 2- Zakup Licencji rocznej na oprogramowanie Microsoft365 Apps for business na 25 stanowisk**

|  |  |
| --- | --- |
| 1 | Licencja CSP zawierająca takie programy jak m. in.: Word, Excel, Outlook, PowerPoint, OneNote, Publisher, Access |
| 2 | Wsparcie techniczne |
| 3 | Zarządzanie licencjami poprzez stronę internetową |

**Zadanie nr 3- Zakup Serwera plikowego do baz danych oraz serwera plikowego do pracy grupowej- 2 szt.**

|  |  |
| --- | --- |
|  | **Serwer plikowy do baz danych oraz serwer plikowy do pracy grupowej** |
| 1 | Obudowa typu RACK, wysokość maksymalnie 2U |
| 2 | System operacyjny Microsoft (możliwość obsługi domeny – licencja) ze wsparciem na min. 4 lata |
| 3 | Procesor min. 6-rdzeniowy |
| 4 | Pamięć RAM: min. 32 GB |
| 5 | Dysk SSD o pojemności min. 6TB, min. 2 szt. z możliwością rozbudowy do 4 szt. |
| 6 | Sprzętowy kontroler RAID |
| 7 | Złącze Ethernet min. 2 szt., złącze USB |
| 8 | Wsparcie wirtualizacji |

**Zadanie 4- Zakup Urządzenia wielofunkcyjnego – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Typ | Urządzenie wielofunkcyjne kolor |
|  | Funkcje | Drukowanie, kopiowanie, skanowanie |
|  | Rozmiar papieru | A3 |
|  | Szybkość wydruku (mono/kolor) | 25/25 str./min. |
|  | Obsługiwane papiery | A3, A4, A5, A6, 80-300 g/m2 |
|  | Obsługa papieru | Podajnik na min. 500 arkuszy A3 i A4 |
|  | Komunikacja | Przewodowa, bezprzewodowa WiFi, USB |
|  | Skanowanie do | e-mail, plik, pamięć USB, udział sieciowy |
|  | Wyświetlacz | Dotykowy, min. 10 cali |
|  | Wymagania dodatkowe | Możliwość ustawienia kont użytkowników z autoryzacją hasłem |

**Zadanie nr 5- Zakup Zasilacza awaryjnego UPS – 25 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Rodzaj | Jednofazowy |
|  | Typ obudowy | Tower |
|  | Technologia | Line-interactive |
|  | Przewód zasilający | Min. 1,5 m |
|  | Moc VA/W | 1000/600 |
|  | Wyjście | 4 gniazda sieciowe zabezbieczone przed przepięciami |
|  | Złącza | 1 x USB, 1 x RJ45 |
|  | Wymagania dodatkowe | Panel LCD, bezpiecznik, uruchamianie na baterii |

**Zadanie nr 6- Zakup** **25 Licencji oprogramowania do szyfrowania wiadomości email technologią END TO END. Wsparcie techniczne i prawo do aktualizacji na 2 lata. Bazy reguł, sygnatur i zagrożeń phishing na 2 lata**

|  |  |
| --- | --- |
| 1. | Oprogramowanie musi zapewnić funkcjonalność: |
| 1.1.    szyfrowanie algorytmem AES256 treści wiadomości, |
| 1.2.    szyfrowanie algorytmem AES256 załączników, |
| 1.3.    szyfrowanie algorytmem AES256 plików, |
| 1.4.    szyfrowanie algorytmem AES256 katalogów, |
| 1.5.    do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego. |
| 1.6.    do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe. |
| 1.7.    do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego. |
| 1.8.    do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego. |
| 1.9.    odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0 |
| 1.10. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki |
| 1.11. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania, |
| 1.12. opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność, |
| 1.13. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem, |
| 1.14. posiadania wewnętrznej bazy haseł, która umożliwia: |
| 1.14.1.     export haseł do pliku, |
| 1.14.2.     import haseł z pliku |
| 1.14.3.     generowania ponownie haseł w bazie |
| 1.15. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich, |
| 1.16. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym, |
| 1.17. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów, |
| 1.18. pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows. |
| 1.19. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym, |
| 1.20. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe, |
| 1.21. wykrywania fałszywych emaili - Antiphishing, |
| 1.22.   wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING, |
| 1.23.   wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych, |
| 1.24.   wykrywanie niebezpiecznych dokumentów MS Office, |
| 1.25.   wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email, |
| 1.26.   definiowania alarmów informujących o niebezpiecznych mailach i załącznikach, |
| 1.27. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlenie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 2 razy w ciągu dnia, |
| 1.28. alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc, |
| 1.29. współpracy z klientem Outlook i Mozilla Thunderbird i Mozilla Thunderbird Portable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11. |
| 2. | Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy. |
| 3. | Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy. |
| 4. | Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami. |
| 5. | Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows. |
| 6. | Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne przez 2 lata. |

**Zadanie nr 7- Zakup** **serwera i oprogramowania zarządzania komputerami przy pomocy kontrolera domeny, wsparcie techniczne i prawo do aktualizacji na 2 lata.**

|  |  |
| --- | --- |
| 1 | **Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:** |
| 1.1.    interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO, |
| 1.2.    system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny, |
| 1.3.    serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS), |
| 1.4.    musi posiadać system antywirusowy, |
| 1.5.    możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3, |
| 1.6.    musi umożliwiać dostęp administratorów przez przeglądarkę WEB, |
| 1.7.    wbudowany firewall zarządzany przez przeglądarkę WEB, |
| 1.8.    przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB, |
| 1.9.    system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB, |
| 1.10. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB, |
| 2 | **W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:** |
| 2.1.    zarządzania do min. 25 użytkowników, grup, |
| 2.2.    zarządzanie do min. 25 komputerów, |
| 2.3.    zarządzanie do min. 25 urządzeń, |
| 2.4.    zarządzania polisami GPO, |
| 2.5.    obsługę profili użytkowników oraz profili mobilnych, |
| 2.6.    obsługę do min. 50 jednoczesnych podłączeń do serwera domeny, |
| 2.7.    zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB, |
| 2.8.    możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB, |
| 2.9.   nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB, |
| 2.10.  wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB, |
| 2.11.    listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB, |
| 2.12. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB, |
| 2.13. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym, |
| 2.14. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego, |
| 2.15.   administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania |
| się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB, |
| 2.16. Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny. |
| 2.17. Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny. |
| 2.18. Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token, |
| 2.19. Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny, |
| 2.20. Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0, |
| 2.21. Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u, |
| 2.22. współpracy z klientami Windows 7,8,8.1,10 w wersji professional |
| 3 | **Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:** |
| 3.1.    obsługę minimum cztero-rdzeniowego procesora, |
| 3.2.    obsługę minimum 32GB RAM-u, |
| 3.3.    obsługę vmware VMDK, |
| 31.4.    obsługę minimum 10 instancji środowisk wirtualnych, |
| 3.5.    zapis stanu maszyny wirtualnej tzw. snapshot, |
| 3.6.    kopii stanu maszyny wirtualnej, |
| 3.7.    emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS, |
| 3.8.    dynamicznej alokacji pamięci na kontener danych |
| 3.9.    współpracy z kontrolerami SATA, SCSI, |
| 3.10.   tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci, |
| 3.11. zarządzanie poprzez przeglądarkę WEB, |
| 3.12. archiwizacje uruchomionych maszyn wirtualnych. |
| 4 | **Oprogramowanie musi również umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista,7,8,8.1,10 w wersji 32 i 64 bity w wersji professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 50 użytkowników i musi realizować:** |
| 4.1.    automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego, |
| 4.2.    automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL, |
| 4.3.    automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego |
| automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego |
|  |  |
|  | **Specyfikacja wdrożenia:** |
| 1 | Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami: |
| 1.1  jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013 i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne, |
| 1.2  jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne. |
| 2 | W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne. |
| 3 | Wdrożenie i szkolenie z oprogramowania musi być realizowane przez certyfikowanych inżynierów z uprawnieniami wystawionymi przez producenta. |
|  |  |
|  | **Serwer główny:** |
| 1 | Obudowa: RACK 1U |
| 2 | [Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie http://www.cpubenchmark.net/high\_end\_cpus.html. Procesor z obsługą wirtualizacji.](http://www.cpubenchmark.net/high_end_cpus.html) |
| 3 | Pamięć: min. 32GB dedykowane do pracy serwerowej |
| 4 | 4 kieszenie HotSwap SATA3 |
| 5 | 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap |
| 6 | 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap. |
| 7 | Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s |
| 8 | Wsparcie KVM przez LAN |
| 9 | Panel przedni chroniący kluczem dostępu do dysków |
| 10 | Czujnik otwarcia obudowy |
| 11 | Komplet szyn montażowych w zestawie |
| 12 | Gwarancja: 2 lata gwarancji producenta |