Załącznik do opisu przedmiotu zamówienia. Część 6

Komputer stacjonarny – 16 sztuk

	Opis minimalnych wymagań
Procesor	Osiągający w testach CPU Benchmark PassMark min. 12400 punktów na dzień 28.04.2021r. Z uwagi na zmienność wyników w/w testu Zamawiający udostępnia w Załączniku nr 1 do załącznika do OPZ Część 6 wyniki na dzień 28.04.2021r. Aktualna lista procesorów i wyników testów jest dostępna pod adresem: https://www.cpubenchmark.net/cpu_list.php Taktowanie w trybie turbo 4,3 GHz Pamięć podręczna 12MB Gwarancja: min 36 miesięcy
Pamięć RAM	16GB DDR4 z możliwością rozbudowy do 32GB 2 gniazda pamięci RAM (1 wolne) Taktowanie 2400 MHz Pamięć zainstalowana i dostarczona przez producenta komputera. Zamawiający nie dopuszcza rozbudowy, modyfikacji, czy zmiany komponentu przez Wykonawcę. Gwarancja: min 60 miesięcy
Porty zewnętrzne (płyta główna)	1x PS/2 4x USB 2.0 2x USB 3.1 3x Audio 1x HDMI 1x VGA 1x RJ-45 1x RS-232 Gwarancja: min 36 miesięcy
Porty i rozszerzenia wewnętrzne	1 x 4-pin wentylator procesora 1 x 4-pin wentylator 1 x 8pin 12V zasilanie 1 x 24pin ATX zasilanie 4 x SATA III 6Gb/s 1 x USB 2.0 1 x USB 3.2 gen. 1 1 x LPT 1 x Clear CMOS zworka 1 x m.2 PCIe 2280 1 x Przedni panel audio 2x PCI-e x1 1x PCI-e x16
Łączność	10/100/1000 Mbps Zamawiający nie dopuszcza stosowania zewnętrznych kart sieciowych lub takich, które wykorzystują którykolwiek z ww. portów na płycie głównej. Karta sieciowa przewodowa, bezprzewodowa oraz Bluetooth muszą być zaimplementowane przez producenta płyty głównej.
Karta graficzna	Karta graficzna 1: Zintegrowana z procesorem. Karta graficzna 2: Osiągający w testach Video Card Benchmark PassMark min. 2600 punktów na dzień 28.04.2021r. Z uwagi na zmienność wyników w/w testu Zamawiający udostępnia w Załączniku nr 2 do załącznika do OPZ Część 6 wyniki na dzień 28.04.2021 r. Aktualna lista kart graficznych i wyników testów jest dostępna pod adresem: https://www.videocardbenchmark.net/gpu_list.php Pamięć 2GB GDDR5 Ilość rdzeni CUDA: 380 Chłodzenie aktywne Posiadająca 2 porty graficzna: 1x HDMI, 1x Displayport Karta graficzna zamontowana i dostarczona przez producenta komputera. Zamawiający nie dopuszcza rozbudowy, modyfikacji, czy zmiany komponentu przez Wykonawcę. Gwarancja: min 36 miesięcy

Dysk	Pojemność: 500GB Format: m.2 Typ: PCI-e x4 3.0 Prędkość odczytu / zapisu: 3100 / 2600 MB/s Ilość operacji odczytu / zapisu IOPS: 400 000 / 470 000 Dysk zainstalowany i dostarczony przez producenta komputera. Zamawiający nie dopuszcza rozbudowy, modyfikacji, czy zmiany komponentu przez Wykonawcę. Gwarancja: min 36 miesięcy
Napęd	Wbudowana nagrywarka DVD+/-RW Zamawiający nie dopuści zewnętrznej nagrywarki jako rozwiązanie równoważne Gwarancja: min 24 miesiące
Obudowa	Obudowa mini Tower przeznaczona do pracy komputera w pionie. Wymiary obudowy nie większe niż: 360 (wys.) x 170 (szer.) x 370 (głęb.) mm. Zamawiający dopuszcza tolerancję w wymiarze obudowy do +2%. Obsługa 4 slotów PCI Posiadająca 1 port USB 3.2 gen. 1 na froncie, 2 porty USB 2.0 na froncie, 2x Audio (in/out) na froncie obudowy Gwarancja: min 24 miesiące
Zasilacz	Moc nie mniejszej niż 500W Sprawności 80+ Bronze Aktywne PFC Zabezpieczenia: UVP (zabezpieczenie podnapięciowe), OVP (zabezpieczenie przeciwprzepięciowe) SCP (zabezpieczenie przeciwzwarciowe) OPP (zabezpieczenie przeciwprzeciążeniowe) SIP (Ochrona przed przepięciami i udarami) Wentylator 14mm MTBF: min. 100 000h Głośność: nie więcej niż 25db Okablowanie: 1x 20+4 PIN ATX; 1x 4+4 PIN 12V, 4x SATA, 2x MOLEX, 1x PIN 6+2 PCI-e Gwarancja: min 24 miesiące
Bezpieczeństwo	Trusted Platform Module (TPM 2.0) Security Chip zintegrowany z obudową lub procesorem
Akcesoria	Klawiatura przewodowa USB z regulowanymi stopkami, antypoślizgowymi, odporna na zachlapanie. Klawiatura niskoprofilowa z wydzieloną klawiaturą numeryczną. Mysz przewodowa USB o rozdzielczości 1000 dpi, posiadająca 3 przyciski, 1 rolkę przewijania. Klawiatura i mysz optyczna w kolorach szarym lub czarnym. Gwarancja: min 24 miesiące
Gwarancja	Min. 24 miesiące gwarancji producenta komputera, czas reakcji 1 dzień roboczy. Za czas reakcji Zamawiający przyjmuje pojawienie się serwisanta producenta komputera lub jego autoryzowanego partnera serwisowego w ciągu 24h od zgłoszenia serwisowego.
System operacyjny	Microsoft Windows 10 Professional PL w wersji komercyjnej lub edukacyjnej. System zainstalowany przez producenta komputera. Zamawiający dopuszcza rozwiązanie równoważne: System zainstalowany przez producenta komputera. Nie wymagający aktywacji za pomocą Internetu lub telefonu. Zainstalowany system operacyjny, w polskiej wersji językowej. Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu. System operacyjny klasy desktop, 64-bit. Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym: 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy; 2) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym: 1) polskim; 2) angielskim. Zlokalizowane w języku polskim, co najmniej następujące elementy:

	1) menu; 2) odtwarzacz multimediów; 3) pomoc; 4) komunikaty systemowe. Wbudowany system pomocy w języku polskim. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. Zintegrowana z systemem operacyjnym konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie. Możliwość pracy systemu w trybie ochrony kont użytkowników. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa /instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, w tym: 1) poziom menu; 2) poziom otwartego okna systemu operacyjnego. Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. Obsługa standardu NFC (near field communication). Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. Mechanizmy logowania do domeny w oparciu o: 1) login i hasło; 2) karty z certyfikatami (smartcard); 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). Mechanizmy wieloelementowego uwierzytelniania. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. Wsparcie dla algorytmów Suite B (RFC 4869). Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2)

	dla warstwy transportowej IPsec. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. Udostępnianie modemu. Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinsatalacji systemu.
Oprogramowanie antywirusowe	
Rodzaj i funkcje	Przeznaczony do kompleksowej ochrony serwerów i stacji klienckich pracujących pod kontrolą systemów z rodziny Microsoft Windows. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.
Czas licencji	Min. 12 miesięcy
Architektura	Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer Oprogramowanie klienckie, zarządzane z poziomu serwera.
Podstawowa funkcjonalność	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci,

	• skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. • Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Szyfrowanie danych: • 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. • 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. • 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
Zarządzanie i administracja	Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • 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 • 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. • 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 • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej
Kontrola urządzeń, aplikacji i DLP	System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth

	• funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi • funkcje blokowania dostępu dowolnemu urządzeniu • możliwość tymczasowego dodania dostępu do urządzenia przez administratora • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx • funkcje monitorowania i kontroli przepływu poufnych informacji • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przez wyciekiem plików poprzez programy typu p2p
Dodatkowe wymagania	Monitorowanie zmian w plikach: • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • Funkcje monitorowania określonych rodzajów plików. • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • Generator raportów do funkcjonalności monitora zmian w plikach. • możliwość śledzenia zmian we wszystkich plikach • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach • możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem

	• możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich • instruktaż stanowiskowy pracowników Zamawiającego • dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: • Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) • Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) • Mac OS X, Mac OS 10 Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat,
Monitor – 16 sztuk	
Rozmiar matrycy	23,8”
Typ matrycy	IPS
Powierzchnia matrycy	Matowa
Rozdzielczość natywna	1920x1080 FHD
Kontrast statyczny	1 000:1
Kontrast dynamiczny	8 000 000:1
Jasność	250 cd/m^2
Poziomy/pionowy kąt widzenia	178/178 stopni
Porty	1x VGA 1x HDMI
Certyfikaty i normy	Energy Star EPEAT RoHS TCO
Gwarancja	Min. 24 miesiące gwarancji producenta
UWAGI OGÓLNE	**ZAMAWIAJĄCY PODAJE PARAMETRY MINIMALNE DLA KAŻDEGO Z PARAMETRÓW OPISU PRZEDMIOTU ZAMÓWIENIA. WYKONAWCY MOGĄ ZAPROPONOWAĆ PARAMETR RÓWNY LUB WYŻSZY NIŻ WYMAGANY PRZEZ ZAMAWIAJĄCEGO. CO ZA TYM IDZIE WYKONAWCA POWINIEN SIĘ KIEROWAĆ WIEDZĄ, DOŚWIADCZENIEM ZAWODOWYM ORAZ LOGIKĄ PRZY OFEROWANIU WYŻSZYCH PARAMETRÓW.**