**Załącznik nr 1 do Umowy**

**Opis Przedmiotu Zamówienia**

|  |  |
| --- | --- |
| **MINIMALNE WYMAGANIA** | |
| **Komputer** | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| **Liczba sztuk** | 30 sztuk |
| **Wydajność komputera** | Oferowany komputer przenośny musi osiągać w teście wydajności :   * SYSMARK 25 – wynik min. 1250 – test z przeprowadzonej konfiguracji załączyć do oferty na wezwanie Zamawiającego. * Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). * Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego. |
| **Ekran** | 15.6” LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową, nie dopuszcza się matryc typu "glare". Klapa komputera otwierana do 180 stopni. |
| **Obudowa** | Waga nie większa niż 1,8kg, grubość nie przekraczająca 20mm. Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium. Obudowa musi spełniać standard MIL-STD 810G (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów). Dopuszczalne kolory – czarny/srebrny. |
| **Chipset** | Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora. |
| **Pamięć operacyjna** | 16GB DDR4 (pamięć RAM rozszerzalna do 32GB). |
| **Dysk twardy** | * Min. 256GB SSD M.2 zawierający partycję RECOVERY – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:   + systemu operacyjnego   + oprogramowania antywirusowego * Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania. * Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5 cala. |
| **Karta graficzna** | Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana. |
| **Audio/Video** | * Wbudowana karta dźwiękowa, zgodna z HD Audio, * Wbudowane głośniki dwa głośniki stereo, * Wbudowane dwa mikrofony. |
| **Karta sieciowa** | Zintegrowana z płytą główną 10/100/1000 – RJ 45 |
| **Porty/Złącza** | * USB 3.2 - 2 szt. * USB Thunderbolt 4 - 1 szt. * USB 2.0 - 1 szt. * HDMI ze wsparciem HDCP - 1 szt. * Czytnik kart pamięci SD lub microSD - 1 szt. * RJ-45 (LAN) - 1 szt. * Wyjście słuchawkowe/wejście mikrofonowe (combo) - 1 szt. * Zasilanie DC-in |
| **Klawiatura** | Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy). |
| **WiFi** | Wbudowana karta sieciowa, pracująca w standardzie AX. |
| **Bluetooth** | Wbudowany moduł Bluetooth 5.0. |
| **Urządzenie wskazujące** | * Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka. * Czytnik linii papilarnych. |
| **Kamera** | Wbudowana, o parametrach:   * HD 1280x720, 720p HD audio/video nagrywanie. * Wbudowane dwa kierunkowe mikrofony. * Mechaniczna przesłona kamery. |
| **Bateria** | Litowo-jonowa min. 41Whr – czas pracy min. 7h wyników testów BAPCO MobileMark 25 – test załączyć do oferty. |
| **Zasilacz** | Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 90W. |
| **Bezpieczeństwo** | * Zabezpieczenie BIOS hasłem użytkownika. * Zabezpieczenie dysku twardego hasłem użytkownika. * Złącze typu Kensington Lock. * Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego - Trusted Platform Module 2.0. |
| **Certyfikaty i standardy** | * Certyfikat ISO 9001, 14001, 50 001 dla producenta sprzętu (należy załączyć do oferty). * Deklaracja zgodności CE i ROHS (załączyć do oferty). * Standard MIL-STD-810G (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów). |
| **Oprogramowanie dodatkowe** | System chroniący przed zagrożeniami. 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. * Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. * Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. * Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. * Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. * Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. * Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. * Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. * Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.   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:   * Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach. * Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury. * Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur. * Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy. * Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach. * Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń. * Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej.   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.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.   1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer. 2. Oprogramowanie klienckie, zarządzane z poziomu serwera.   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   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   Platforma do zarządzania dla Android i iOS:   * Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę * Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. * Zarządzanie użytkownikiem * Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email * Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika * Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi * Musi posiadać możliwość eksportu danych użytkownika   Zarządzanie urządzeniem:   * Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO * Musi umożliwiać import listy urządzeń z pliku CSV * Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych * Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta * Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał * Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres * Musi zawierać podgląd aktualnie zainstalowanych aplikacji * Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, * Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł * Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres.   Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:   1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:    * Microsoft Internet Explorer    * Microsoft Edge    * Mozilla Firefox    * Google Chrome    * Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:    * Windows 2008 R2    * Windows 2012    * Windows 2012 R2    * Windows 2016 7. Portal zarządzający musi umożliwiać:  * przegląd wybranych danych na podstawie konfigurowalnych widgetów * zablokowania możliwości zmiany konfiguracji widgetów * zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. * tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności * eksport wszystkich skanów podatności do pliku CSV |
| **System operacyjny** | Windows 10 Professional 64 bit lub równoważny;  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   * Dostępne dwa rodzaje graficznego interfejsu użytkownika:   + Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,   + Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych * Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. * Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. * Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. * Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. * Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. * Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. * Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. * Wbudowany system pomocy w języku polskim. * Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). * Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. * Klucz produktu przypisany do komputera aby przy ponownej reinstalacji systemu nie było konieczności wpisywania klucza. * Możliwość podłączenia do domeny Active Directory.   W formularzu oferty trzeba podać nazwę oferowanego oprogramowania. |
| **Diagnostyka** | System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia: dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu: pamięć flash, USBpen itp. |
| **Gwarancja** | * Gwarancja producenta komputera min. 36 miesięcy * Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta * Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera. * Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001 * Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych. |
| **Wsparcie techniczne** | * Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. * W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji. |
| **Pozostałe** | Sprzęt ma być fabrycznie nowy tj. nieużywany, nieuszkodzony, nieregenerowany, nieobciążony prawami osób lub podmiotów trzecich i wyprodukowany nie wcześniej niż na 24 miesiące przed terminem składania ofert oraz pochodzić z legalnego kanału sprzedaży producenta. Wszystkie sztuki laptopów muszą pochodzić od jednego producenta. |