*Załącznik nr 6*

Dotyczy zapytania ofertowego nr **1/02/2022/PDKZ**. w ramach projektu **„Plus dla kształcenia zawodowego”** współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.  
  
**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:**

Przedmiotem zamówienia jest dostawa wraz z montażem wskazanego sprzętu technologii informacyjno– komunikacyjnej stanowiący doposażenia pracowni szkolnych:

**Poz. 1 Komputer stacjonarny – ilość szt. 16**Kod CPV: 30213000-5

**Poz. 2 Klawiatura komputerowa – ilość szt. 16**Kod CPV: 30237460-1

**Poz. 3 Monitor komputerowy – ilość szt. 16**Kod CPV: 30231300-0

**Poz. 4 Mysz komputerowa – ilość szt. 16**Kod CPV: 30237410-6

|  |  |
| --- | --- |
| Nazwa komponentu | Wymagane parametry techniczne komputerów |
| Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| Wydajność obliczeniowa | Procesor dedykowany do pracy w komputerach stacjonarnych.  Oferowany komputer musi osiągać w teście wydajności :  SYSMARK 25 Overall Rating – wynik min. 1300 pkt – test z przeprowadzonej konfiguracji załączyć do oferty.  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.) |
| Pamięć RAM | Minimum 16GB DDR4 o częstotliwości taktowania min 2666MHz. Możliwość rozbudowy do min 64GB. Minimum jeden slot DIMM wolny. |
| Pamięć masowa | Dysk M.2 SSD PCIe NVMe o pojemności min. 256GB |
| Wydajność grafiki | Zintegrowana z procesorem |
| Wyposażenie multimedialne | Karta dźwiękowa min. czterokanałowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out. |
| Obudowa | Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki. Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Bezpieczeństwo | System diagnostyczny z graficznym interfejsem użytkownika, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy.  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. 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, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. 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.  Zamawiający wymaga fabrycznie nowego systemu operacyjnego, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu.  Zamawiający wymaga, aby oprogramowanie systemowe było fabrycznie zainstalowane przez producenta komputera.  Zamawiający wymaga, aby oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności, np. tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) stosowanymi przez producenta sprzętu lub inną formą uwiarygodniania oryginalności wymaganą przez producenta oprogramowania stosowną w zależności od dostarczanej wersji.  Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania w przypadku wystąpienia wątpliwości, co do jego legalności. |
| Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + lub równoważny. Silnik musi umożliwiać co najmniej:  • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają w 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:  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  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  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  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:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV |
| Certyfikaty i standardy | * Deklaracja zgodności CE (załączyć do oferty) * Urządzenia muszą być wyprodukowane zgodnie z normą PN-EN ISO 50001 oraz ISO 9001 lub posiadać równoważny certyfikat na świadczenie usług serwisowych oraz serwis urządzeń musi być realizowany przez producenta – wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta (należy dołączyć do oferty). * Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A.)lub certyfikat równoważny. * Certyfikat WHQL dla systemu operacyjnego lub równoważny. |
| Wymagania dodatkowe | Minimalne wymagania dot. portów: 1 x HDMI 1.4, 1 x VGA, port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu, port audio-out na tylnym panelu obudowy, 1xRJ-45, 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie:  - Panel przedni: min. 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0  - Panel tylny: min. 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona minimalnie w:  1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0.  Minimum jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej.  Klawiatura USB w układzie polski programisty  Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)  Wbudowana nagrywarka DVD +/-RW |
| Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego  - Naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| Warunki gwarancji | Co najmniej 3-letnia gwarancja producenta świadczona na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych lub równoważny certyfikat na świadczenie usług serwisowych~~,~~ serwis urządzeń musi być realizowany przez producenta –dokumenty potwierdzające załączyć na wezwanie zamawiającego  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) |
| Monitor | Wyświetlacz: min. 21,5” IPS, Rozdzielczość: min. 1920x1080 Full HD  Jasność: min. 250 cd/m2  Kontrast statyczny min. 1000:1  Plamka maks.: 0,250mm  Technologie: Flicker free, Filtr światła niebieskiego  Pochylenie min. od -5 do +23 stopni  Wbudowane VESA min. 100x100  Wbudowane złącza: min. 1x HDMI, 1x VGA  Czas reakcji: mak. 5 ms (szary do szarego)  Gwarancja min. 36 miesięcy |
| Dodatkowe oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Oprogramowanie zarządzające producenta komputera, instalowane na etapie produkcji komputera, umożliwiające min.:  - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów  - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu  - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów  - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.  Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o:   + poprawkach i usprawnieniach dotyczących aktualizacji   + dacie wydania ostatniej aktualizacji   + priorytecie aktualizacji   + zgodności z systemami operacyjnymi   + jakiego komponentu sprzętu dotyczy aktualizacja   + wszystkich poprzednich aktualizacjach z informacjami jak powyżej. * wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne * możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. * rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr ) * sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr) i wersją (rewizja wydania) * dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml * raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
| Oprogramowanie biurowe | Pakiet aplikacji biurowych dla uczniów, spełniający poniższe wymagania:  - Dostępny w architekturze 64-bitowej i 32-bitowej  - Oferowany w polskiej wersji językowej,  - Licencja bezterminowa  Pakiet aplikacji biurowych musi spełniać następujące wymagania minimalne:  - Pakiet biurowy dostarczony wraz z licencją i nośnikiem.  - Wymagania odnośnie interfejsu użytkownika:  - Pełna polska wersja językowa interfejsu użytkownika.  - Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.  - Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.  Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:  - posiada kompletny i publicznie dostępny opis formatu,  - ma zdefiniowany układ informacji w postaci XML,  - umożliwia wykorzystanie schematów XML, wspiera w swojej specyfikacji podpis elektroniczny.  Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.  W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy),  Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.  Pakiet zintegrowanych aplikacji biurowych musi zawierać:  - Edytor tekstów  - Arkusz kalkulacyjny  - Narzędzie do przygotowywania i prowadzenia prezentacji  - Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)  Edytor tekstów musi umożliwiać:  - Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.  - Wstawianie oraz formatowanie tabel i obiektów graficznych.  - Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  - Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków oraz tworzenie spisów treści.  - Formatowanie nagłówków i stopek stron.  - Sprawdzanie pisowni w języku polskim.  - Śledzenie zmian wprowadzonych przez użytkowników.  - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  - Określenie układu strony (pionowa/pozioma).  - Wydruk dokumentów.  - Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  - Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów Dokumentu.  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  - Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.  - Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.  - Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.  Arkusz kalkulacyjny musi umożliwiać:  - Tworzenie raportów tabelarycznych i wykresów liniowych (wraz linią trendu), słupkowych, kołowych.  - Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.  - Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).  - Obsługę „kostek OLAP” oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.  - Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.  - Wyszukiwanie i zamianę danych.  - Wykonywanie analiz danych przy użyciu formatowania warunkowego.  - Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.  - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  - Formatowanie czasu, daty i wartości finansowych z polskim formatem.  - Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  - Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010 i 2013 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  - Przygotowywanie prezentacji multimedialnych, które będą:  a) Prezentowane przy użyciu projektora multimedialnego.  b) Drukowane w formacie umożliwiającym robienie notatek.  c) Zapisane jako prezentacja tylko do odczytu.  - Nagrywanie narracji i dołączanie jej do prezentacji.  - Opatrywanie slajdów notatkami dla prezentera.  - Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.  - Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.  - Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.  - Możliwość tworzenia animacji obiektów i całych slajdów.  - Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.  - Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007 2010 i 2013.  - Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  - Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.  - Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.  - Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.  - Automatyczne grupowanie poczty o tym samym tytule.  - Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.  - Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia.  - Zarządzanie kalendarzem.  - Udostępnianie kalendarza innym użytkownikom.  - Przeglądanie kalendarza innych użytkowników.  - Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.  - Zarządzanie listą zadań.  - Zlecanie zadań innym użytkownikom.  - Zarządzanie listą kontaktów.  - Udostępnianie listy kontaktów innym użytkownikom.  - Przeglądanie listy kontaktów innych użytkowników.  - Możliwość przesyłania kontaktów innym użytkowników.  Zamawiający wymaga fabrycznie nowego oprogramowania biurowego, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu.  Zamawiający wymaga, by oprogramowanie biurowe było fabrycznie zainstalowane przez producenta komputera. |