**Załącznik 5**

|  |  |
| --- | --- |
| **D. KALKULACJA CENY** | |
| **Nazwa zamówienia** | **„Zakup i dostawa (wraz z rozładunkiem) wyposażenia i sprzętu informatycznego do pracowni w szkołach podstawowych i szkołach podstawowych specjalnych w podziale na części w ramach projektu Wiele potrzeb- jeden cel”.**  **Część III:**  **„Zakup i dostawa (wraz z rozładunkiem) laptopów do pracowni w ramach projektu „Wiele potrzeb- jeden cel”** |
| **Nazwa Wykonawcy** |  |
| **Adres Wykonawcy** |  |

**Laptopy - 18 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa podzespołu/ parametry** | **Opis minimalnych wymagań** | **Opis oferowanego podzespołu – proszę wpisać parametry (nazwy, typy, warianty, producenta)**  *(wypełnia Wykonawca)* |
| **Producent, model i numer katalogowy oferowanego sprzętu ……………………………………..(wypełnić)** | |  |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |  |
| Przekątna Ekranu | Min. 15.6 FHD (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nits  Kąt otwarcia matrycy min.180 stopni |  |
| Wydajność | Oferowany komputer przenośny musi osiągać w teście wydajności: SYSMARK 2018- wynik min. 1140- potwierdzone wydrukiem z systemu;  MobileMARK 2018- wynik min. 900- potwierdzone wydrukiem z systemu |  |
| Procesor | Procesor osiąga w teście PassMark Performance Test CPU Mark z dnia, który mieści się w przedziale od ogłoszenia do dnia składania oferty, co najmniej 6000 punktów w Passmark CPU Mark. Dostępny na stronie: http://www.passmark.com/ |  |
| Pamięć RAM | Min. 8GB DDR4 2400MH z możliwością rozbudowy do max. 20GB RAM. |  |
| Pamięć masowa | Min. 256GB NVMe SSD M.2  Laptop musi mieć możliwość zainstalowania drugiego dysku w przyszłości. |  |
| Karta graficzna | Zintegrowana karta graficzna osiągająca w teście PassMark Performance Test z dnia, który mieści się w przedziale od ogłoszenia do dnia składania oferty, co najmniej 1000 punktów w G3D Rating. Dostępny na stronie: http://www.videocardbenchmark.net/ |  |
| Klawiatura | (układ US), min 100 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. |  |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo 2x2W.  Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.  Kamera internetowa z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy.  1 port audio typu combo (słuchawki i mikrofon) |  |
| Łączność bezprzewodowa | Intel® lub równoważny Wi-Fi 5 AC 201 2x2 + Bluetooth 4.2 |  |
| Bateria i zasilanie | Bateria Polymer min. 2-cell [min. 36Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie max. 1 godziny i do poziomu 100% w czasie max. 2 godzin.  Czas pracy na baterii min 5 godzin, potwierdzony przeprowadzonym testem MobileMark 2018 Battery Life  Zasilacz o mocy min. 65W |  |
| Waga i wymiary | Waga max 1.9 kg z baterią  Wysokość laptopa nie większa niż 20mm. |  |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem  i wilgocią. |  |
| 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 równoważne. SystemSystem 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 ma 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 |  |
| 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. |  |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia  i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych  na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. |  |
| System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Zainstalowany system operacyjny MS Windows 10 Professional 64bit PL lub równoważne, spełniające poniższe warunki:  1. System operacyjny z graficznym interfejsem użytkownika,  2. System operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016,2019;  3. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,  4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,  5. Wbudowany system pomocy w języku polskim,  6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,  7. 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,  8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,  9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,  10. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,  12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),  13. Wsparcie dla urządzeń peryferyjnych typu maty interaktywne, monitory interaktywne,  14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,  15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe- przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,  16. Rozbudowane, definiowalne polityki bezpieczeństwa- polityki dla systemu operacyjnego i dla wskazanych aplikacji,  17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,  18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  19. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów:  I. poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty  na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.  22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  24. Mechanizmy logowania do domeny w oparciu o:  a. Login i hasło,  b. Karty z certyfikatami (smartcard),  c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  25. Mechanizmy wieloelementowego uwierzytelniania.  26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,  27. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,  28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  29. Wsparcie dla środowisk Java i .NET Framework 4.x- możliwość uruchomienia aplikacji działających we wskazanych środowiskach,  30. Wsparcie dla JScript i VBScript- możliwość uruchamiania interpretera poleceń,  31. Zdalna pomoc i współdzielenie aplikacji– możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu  z komputerem,  32. 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,  33. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,  34. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność  i pozwalający tworzyć kopie zapasowe,  35. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.  36. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,  37. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,  38. 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.),  39. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),  40. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,  41. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,  42. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.  43. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych  44. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.  45. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu |  |
| Oprogramowanie biurowe | Pakiet biurowy wraz z licencjami i kluczami instalacyjnymi na pojedyncze stanowiska typu Microsoft Office 2019 lub równoważny zawierający wszystkie składowe programy w jednym pakiecie w ramach jednego producenta, co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji multimedialnych, program do obsługi poczty elektronicznej oraz kalendarza, które charakteryzuje się następującymi cechami:  - całkowicie zlokalizowany w języku polskim interfejs, system komunikatów i podręcznej kontekstowej pomocy technicznej (w tym także on-line) w pakiecie, (całkowicie oryginalna polska licencja, Zamawiający nie dopuszcza zaoferowania licencji innej niż polska)  - możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego),  - możliwość zdalnej instalacji komponentów,  - możliwość prowadzenia dyskusji oraz subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach, oraz publikowanie dokumentów wprost z komponentów pakietu np. arkusza kalkulacyjnego,  - w systemach pocztowych- możliwość delegacji uprawnień do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji,  możliwość blokowania niebezpiecznej lub niechcianej poczty,  - automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi, potwierdzanie dostarczenia do skrzynki adresata oraz potwierdzanie otwarcia poczty u adresata,  - współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników,  - wsparcie dla formatu XML w podstawowych aplikacjach,  możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów,  - automatyczne wyróżnianie i aktywowanie hyperlinków w dokumentach podczas edycji i odczytu,  - możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych,  - możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/ arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony,  - możliwość zaszyfrowania danych w dokumentach i arkuszach kalkulacyjnych zgodnie ze standardem CryptoAPI,  - możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu,  - prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach:.doc, .docx, xls,.xlsx, ppt, .pptx, .pps, .ppsx, w tym obsługa formatowania, wykonywanie i edycję makr oraz kodu zapisanego w języku Visual Basic for Application w plikach xls, xlsx, formuł, formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013 bez utraty danych oraz bez konieczności reformatowania dokumentów,  - prawidłowe otwieranie i zapisywanie plików o formatach doc, docx, xls, xlsx, .ppt, pptx. .pps, .ppsx bez utraty parametrów i cech użytkowych zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów, działające makra,  - prawidłowa współpraca zapis, odczyt z plikami danych programów pocztowych w formacie .pst oraz prawidłowy import z formatu .dbx,  - wszystkie komponenty oferowanego pakietu biurowego (edytor, arkusz, klient poczty, kalendarz oraz program do prezentacji) muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi,  - poprawna praca w systemach operacyjnych w które może być wyposażony zamawiany zestaw, tj. 64-bitowych z rodziny Windows 10 lub równoważny,  - w przypadku zaoferowanego oprogramowania równoważnego należy podać dokładną nazwę i wersję oferowanego produktu,  Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.  Zamawiający wymaga, aby wszystkie elementy pakietu biurowego oraz jego licencja pochodziły od tego samego producenta. |  |
| Porty i złącza | Wbudowane porty i złącza:  1x HDMI 1.4 lub nowszy,  1x RJ-45,  3x USB Typ-A w tym min. 1x USB 3.1 lub nowszy,  port zasilania, złącze linki zabezpieczającej, |  |
| Warunki gwarancyjne, wsparcie techniczne | **Bezpłatna gwarancja minimum 36 miesięcy.** Gwarancja musi oferować przez cały okres:  - opiekę kierownika technicznego ds. Eskalacji;  - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze);  Dedykowany portal techniczny producenta,  umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Czas reakcji serwisu- do końca następnego dnia roboczego. |  |

**Podsumowanie dla części III:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Przedmiot zamówienia | Ilość sztuk/zestawów | Cena jednostkowa netto | Wartość netto | Stawka VAT | Kwota VAT | Cena brutto |
| ***1.*** | ***2.*** | ***3.*** | ***4.*** | ***5.*** | ***6.*** | ***7.*** | ***8.*** |
|  | **Laptop** | **18** |  |  | **23%** |  |  |
|  | **Razem brutto** | | | | | |  |

***DOKUMENT NALEŻY PODPISAĆ ELEKTRONICZNIE***