#### **Załącznik nr 4 do SWZ- część 1**

**Opis przedmiotu zamówienia**

dot. zakupu wyposażenia (dostawa i montaż) pracowni komputerowej   
na potrzeby projektu pn. „Energia kwalifikacji – Energia rozwoju” w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020, Osi priorytetowej 10. Innowacyjna edukacja, Działania 10.2 Kształcenie ogólne i zawodowe, Poddziałania 10.2.3 Kształcenie zawodowe.

1. **Komputer stacjonarny – 15 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ | Komputer stacjonarny. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Wydajność | Oferowany komputer przenośny musi osiągać w teście wydajności SYSMARK 2018 Overall rating, wynik 1300 pkt.  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 |
| Procesor | Musi osiągać wynik 13 700 w teście PassMark Average CPU Mark. |
| Pamięć operacyjna | 16 GB DDR4 2400MHz, możliwość rozbudowy do 64GB, minimum 2 sloty wolne na dalszą rozbudowę. Obsługa pamięci OC DDR4-4400 MHz. |
| Parametry pamięci masowej | 512GB SSD |
| Grafika | Ze wsparciem dla DirectX 11, ShaderModel 5.0, OpenGL 3.2 |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, 2 kanałowa; |
| Obudowa | Obudowa o sumie wymiarów nie większej niż 100cm.  Możliwość montażu pełnowymiarowych kart graficznych, montaż beznarzędziowy dysku 3,5" oraz 2,5”, napędu optycznego i kart rozszerzeń. Obudowa wykonana z wytrzymałego tworzywa, blachy o grubości co najmniej 0,5 mm.  Możliwość montażu dysku 2,5" oraz 3,5" wewnątrz obudowy  Zatoki na dyski i napędy: 4× 2,5", 2× 2,5/3,5", 1× 3,5, 2 x 5,25”.  Wyposażona w 2 porty 3.1 oraz złącza mikrofonu i słuchawek z przodu obudowy  Wbudowana karta sieciowa 10/100/1000  Możliwość otwierania bez użycia narzędzi (wkręty ręczne)  Wyposażona w Kensington Lock i ucho na kłódkę  Zasilacz o mocy minimum 500W;  Zamontowane trzy fabrycznie filtry przeciwkurzowe, umiejscowione na froncie, pod zasilaczem oraz na topie obudowy.  Obudowa wyposażona w trzystopniowy kontroler obrotów na w sumie 6 wentylatorów |
| Certyfikaty i standardy | Komputer musi być wyprodukowany zgodnie z normami ISO 9001, ISO 27001, ISO 28000. |
| BIOS | 1. BIOS zgodny ze specyfikacją UEFI 2. Możliwość obsługi klawiaturą oraz myszą 3. Możliwość, bez uruchamiania systemu operacyjnego odczytania z BIOS informacji o: 4. wersji BIOS, 5. nr seryjnym komputera, 6. ilości pamięci RAM, 7. typie procesora, 8. pojemności zainstalowanego dysku twardego 9. rodzajach napędów optycznych 10. kontrolerze audio 11. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego 12. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń |
| Wymagania dodatkowe | 1. Wbudowane porty: 2. 1 x DisplayPort, 3. 1 x HDMI ver. 1.4 4. 8 portów USB wyprowadzonych na zewnątrz komputera w tym 2 porty USB 3.1 z przodu obudowy, 4szt. USB 3.1 z tyłu obudowy oraz 1szt. USB Type-C. Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp. 5. porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. 6. Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n 7. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL, PXE 2.1. 8. Płyta główna zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości., przeznaczona dla danego urządzenia; wyposażona w : 9. SATA III (6 Gb/s) - 6 szt. 10. M.2 - 3 szt. 11. PCIe 3.0 x16 - 2 szt. 12. PCIe 3.0 x1 - 4 szt. 13. 4 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, z obsługą DDR4-4400 MHz 14. Klawiatura USB w układzie polski programisty 15. Mysz USB z klawiszami oraz rolką (scroll) 16. Wbudowana w obudowę nagrywarka DVD +/-RW szybkość x24 wraz z oprogramowaniem do nagrywania i odtwarzania płyt 17. Wsparcie dla konfiguracji RAID 18. Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera. 19. System zasilania chroniący obwód specjalnie zaprojektowany przez producenta płyty głównej z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo złych zasilaczy. |
| Warunki gwarancyjne | 3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w języku polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 11. Graficzne środowisko instalacji i konfiguracji w języku polskim 12. Wbudowany system pomocy w języku polskim. 13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 18. Konta i profile użytkowników zarządzane zdalnie; 19. Praca systemu w trybie ochrony kont użytkowników. 20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 21. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 25. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 30. Wbudowany mechanizm wirtualizacji typu hypervisor; 31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 42. Możliwość tworzenia wirtualnych kart inteligentnych. 43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 44. Wsparcie dla IPSEC oparte na politykach; 45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 46. Mechanizmy logowania w oparciu o: 47. Login i hasło, 48. Karty inteligentne i certyfikaty (smartcard), 49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 50. Umozliwiajacy pracę w domenie; |
| Oprogramowanie zabezpieczające i diagnostyczne | 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny; 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci 7. 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. 8. 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. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; 27. Konsola zarządzająca musi umożliwiać co najmniej: 28. przechowywanie danych w bazie typu SQL; 29. zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; 30. tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; 31. centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. 32. raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; 33. definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 34. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych   zainstalowanych w różnych lokalizacjach;   1. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 2. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 3. Musi posiadać dostęp do konsoli z dowolnego miejsca; 4. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 5. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 6. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych; 7. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 8. Konsola systemu musi umożliwiać, co najmniej: 9. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie 10. przyznanie praw dostępu dla nośników pamięci tj. USB, CD 11. regulowanie połączeń WiFi i Bluetooth 12. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe 13. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi 14. blokowanie dostępu dowolnemu urządzeniu 15. tymczasowe dodania dostępu do urządzenia przez administratora 16. szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; 17. zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka 18. zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora 19. używanie tylko zaufanych urządzeń sieciowych; 20. Wirtualna klawiatury 21. Możliwość blokowania każdej aplikacji 22. Możliwość zablokowania aplikacji w oparciu o kategorie 23. Możliwość dodania własnych aplikacji do listy zablokowanych 24. Dodawanie aplikacji w formie portable 25. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 26. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 27. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 28. Możliwość zablokowania funkcji Printscreen 29. Monitorowania przesyłu danych między aplikacjami; 30. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 31. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 32. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 33. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 34. Ochrona zawartości schowka systemu 35. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 36. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 37. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 38. Możliwość tworzenia profilu DLP dla każdej polityki 39. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 40. Ochrona przez wyciekiem plików poprzez programy typu p2p 41. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 42. Monitorowanie określonych rodzajów plików. 43. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 44. Możliwość śledzenia zmian we wszystkich plikach 45. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 46. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 47. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 48. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 49. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 50. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 51. Musi posiadać możliwość eksportu danych użytkownika 52. Musi umożliwiać import listy urządzeń z pliku CSV 53. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 54. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 55. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; 56. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 57. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 58. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 59. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 60. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: 61. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 62. Portal musi być dostępny w postaci usługi hostowanej; 63. Skanowanie podatności za pomocą nodów skanujących 64. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 65. Portal zarządzający musi umożliwiać: 66. przegląd wybranych danych na podstawie konfigurowalnych widgetów 67. zablokowanie możliwości zmiany widgetów 68. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. 69. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności 70. eksport wszystkich skanów podatności do pliku CSV;   Oprogramowanie producenta komputera umożliwiające zdalną i lokalną administrację oferowanych komputerów oraz ich diagnostykę, pozwalające na:   1. zdalną i lokalną inwentaryzację komponentów komputera 2. zdalne i lokalne monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS 3. zdalne włączenie, wyłączanie oraz restart komputera w sieci, 4. monitorowanie i alertowanie temperatur, napięć i zajętości dysków twardych wraz z wykresami; 5. Interfejs komunikacyjny w języku polskim; 6. w celu zapewnienia pełnej kompatybilności ww. oprogramowania z komputerem, musi być ono wyprodukowane w całości przez producenta komputera; |
| Oprogramowanie biurowe | Zainstalowane oprogramowanie biurowe- kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Wymagania odnośnie interfejsu użytkownika: 2. Pełna polska wersja językowa interfejsu użytkownika; 3. Prostota i intuicyjność obsługi, pozwalająca na prace osobom   nieposiadającym umiejętności technicznych;   1. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się; 2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki: 3. posiada kompletny i publicznie dostępny opis formatu, 4. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) 5. umożliwia wykorzystanie schematów XML 6. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) 7. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców; 8. Zamawiający wymaga licencji przeznaczonych wyłącznie dla jednostek edukacyjnych; 9. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami; 10. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;. 11. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 12. Edytor tekstów 13. Arkusz kalkulacyjny 14. Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji 15. Narzędzie do zarzadzania informacja prywata (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) 16. Edytor tekstu musi umożliwiać: 17. Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty 18. Wstawianie oraz formatowanie tabel 19. Wstawianie oraz formatowanie obiektów graficznych 20. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne) 21. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków 22. Automatyczne tworzenie spisów treści 23. Formatowanie nagłówków i stopek stron 24. Sprawdzanie pisowni w języku polskim 25. Śledzenie zmian wprowadzonych przez użytkowników 26. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności 27. Określenie układu strony (pionowa/pozioma) 28. Wydruk dokumentów 29. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną 30. Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu 31. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 32. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. 33. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. 34. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. 35. Arkusz kalkulacyjny musi umożliwiać: 36. Tworzenie raportów tabelarycznych 37. Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych 38. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. 39. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) 40. Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych 41. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych 42. Wyszukiwanie i zamianę danych 43. Wykonywanie analiz danych przy użyciu formatowania warunkowego 44. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie 45. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności 46. Formatowanie czasu, daty i wartości finansowych z polskim formatem 47. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. 48. Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.. 49. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 50. Narzędzie do projektowania i pracy z lokalnymi bazami danych, tego samego producenta, co reszta programów zawartych w oprogramowaniu biurowym; 51. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz: 52. Prezentowanie przy użyciu projektora multimedialnego 53. Drukowanie w formacie umożliwiającym robienie notatek 54. Zapisanie w postaci tylko do odczytu. 55. Nagrywanie narracji dołączanej do prezentacji 56. Opatrywanie slajdów notatkami dla prezentera 57. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo 58. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego 59. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym 60. Tworzenie animacji obiektów i całych slajdów 61. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera 62. Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016. 63. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać: 64. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego 65. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców 66. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną 67. Automatyczne grupowanie poczty o tym samym tytule 68. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy 69. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia 70. Zarzadzanie kalendarzem 71. Udostępnianie kalendarza innym użytkownikom 72. Przeglądanie kalendarza innych użytkowników 73. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach 74. Zarzadzanie lista zadań 75. Zlecanie zadań innym użytkownikom 76. Zarzadzanie listą kontaktów 77. Udostępnianie listy kontaktów innym użytkownikom 78. Przeglądanie listy kontaktów innych użytkowników 79. Możliwość przesyłania kontaktów innym użytkowników |

1. **Monitor – 15 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Rozmiar | 23,8 cala; |
| Typ panelu | VA |
| Podświetlenie | W-LED |
| Powłoka ekranu | Przeciwodblaskowa, 3H; |
| Format obrazu | 16:9 |
| Rozdzielczość | 1920 x 1080 |
| Czas reakcji matrycy | Maksymalnie 5 ms. |
| Jasność | 250  cd/m² |
| Kontrast | 3000:1 |
| Rozmiar plamki | Maksymalnie 0,28 x 0,28 mm; |
| Katy widzenia | * 178 stopni; |
| Złącza | VGA, HDMI, wyjście audio, |
| Głośniki wbudowane | 2 x 2W; |
| Pochylenie | -5 do 20 stopni; |
| Pobór mocy | Maksymalnie 15W; |
| Warunki gwarancji | 3 lata; |
| Wymagania dodatkowe | Blokada kansington, zgodnośc ze standardem VESA, kabel HDMI; |

1. **Komputer dla nauczyciela z monitorem i oprogramowaniem – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Zastosowanie | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. |
| Ekran | 15.6” LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową;  Klapa komputera otwierana do 150 stopni. |
| Wydajność | Oferowany komputer przenośny musi osiągać w teście wydajności SYSMARK 2018 Overall rating, wynik 1600 pkt.  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 |
| Pamięć RAM | 32 GB DDR4 2666 Mhz; |
| Parametry pamięci masowej | 512GB SSD.  Dysk twardy musi zawierać partycję recovery.  Na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych:   1. systemu operacyjnego 2. oprogramowania zbezpieczającego;   Partycja musi zapewniać przywróceniaw/w oprogramowania.  Możliwość isntalacji trzech wewnętrznych dysków twardych, poza dyskiem systemowym dodatkowo: dysk 2.5 oraz M.2 NVMe |
| Grafika | Oferowany komputer przenośny musi osiągać w teście wydajności SYSMARK 2018 Creativity, wynik 2000 pkt.  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 |
| Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz cyfrowy mikrofon |
| Wbudowane połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LAN  WLAN 802.11 ax/a/b/g/n wraz z Bluetooth 5.1 |
| Porty/złącza  (wbudowane) | 1x Złącze RJ-45;  1x USB 3.2 typ-C;  2x USB 3.2  1x USB 2.0  1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)  1x HDMI 2.0 ze wsparciem HDCP  1x zasilanie DC-in |
| Klawiatura | Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi 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).  Klawiatura typu CHICLET. |
| Urządzenie wskazujące | Touch Pad wbudowany w obudowę notebooka. |
| Kamera | Wbudowana, HD 1280x720.  Wbudowane dwa kierunkowe mikrofony. |
| Bateria | Litowo-jonowa 3 komorowa 48Whr;  Czas pracy na baterii - 6h według wyników testów BAPCO MobileMark 2018 Battery Life. |
| Zasilacz | Zewnętrzny, o mocy maksymalnej 180W; |
| Obudowa waga i wymiary | Waga maksymalnie 2 kg.;  Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium.  Obudowa musi spełniać standard MIL-STD 810G lub 810H (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów) |
| Bezpieczeństwo | 1. Zabezpieczenie BIOS hasłem użytkownika. 2. Zabezpieczenie dysku twardego hasłem użytkownika. 3. Złącze typu Kensington Lock. 4. TPM 2.0. |
| Certyfikaty i standardy | Komputer musi być wyprodukowany zgodnie z normami ISO 9001, 14001.  Komputer musi być wyprodukowany zgodnie ze standardem MIL-STD-810G lub 810H |
| Wsparcie techniczne producenta | 1. Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta, realizowany poprzez podanie na stronie internetowej producenta komputera numeru seryjnego lub modelu komputera; 2. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu darmowego oprogramowania lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. 3. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez producenta były przez niego certyfikowane. |
| Gwarancja | Gwarancja - 36 miesięcy, w tym na baterię - 12 miesięcy; |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w języku polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 11. Graficzne środowisko instalacji i konfiguracji w języku polskim 12. Wbudowany system pomocy w języku polskim. 13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 18. Konta i profile użytkowników zarządzane zdalnie; 19. Praca systemu w trybie ochrony kont użytkowników. 20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 21. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 25. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 30. Wbudowany mechanizm wirtualizacji typu hypervisor; 31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 42. Możliwość tworzenia wirtualnych kart inteligentnych. 43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 44. Wsparcie dla IPSEC oparte na politykach; 45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 46. Mechanizmy logowania w oparciu o: 47. Login i hasło, 48. Karty inteligentne i certyfikaty (smartcard), 49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 50. Umozliwiajacy pracę w domenie; |
| Oprogramowanie zabezpieczające | 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny; 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci 7. 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. 8. 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. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; 27. Konsola zarządzająca musi umożliwiać co najmniej: 28. przechowywanie danych w bazie typu SQL; 29. zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; 30. tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; 31. centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. 32. raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; 33. definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 34. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych   zainstalowanych w różnych lokalizacjach;   1. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 2. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 3. Musi posiadać dostęp do konsoli z dowolnego miejsca; 4. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 5. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 6. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych; 7. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 8. Konsola systemu musi umożliwiać, co najmniej: 9. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie 10. przyznanie praw dostępu dla nośników pamięci tj. USB, CD 11. regulowanie połączeń WiFi i Bluetooth 12. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe 13. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi 14. blokowanie dostępu dowolnemu urządzeniu 15. tymczasowe dodania dostępu do urządzenia przez administratora 16. szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; 17. zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka 18. zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora 19. używanie tylko zaufanych urządzeń sieciowych; 20. Wirtualna klawiatury 21. Możliwość blokowania każdej aplikacji 22. Możliwość zablokowania aplikacji w oparciu o kategorie 23. Możliwość dodania własnych aplikacji do listy zablokowanych 24. Dodawanie aplikacji w formie portable 25. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 26. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 27. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 28. Możliwość zablokowania funkcji Printscreen 29. Monitorowania przesyłu danych między aplikacjami; 30. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 31. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 32. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 33. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 34. Ochrona zawartości schowka systemu 35. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 36. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 37. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 38. Możliwość tworzenia profilu DLP dla każdej polityki 39. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 40. Ochrona przez wyciekiem plików poprzez programy typu p2p 41. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 42. Monitorowanie określonych rodzajów plików. 43. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 44. Możliwość śledzenia zmian we wszystkich plikach 45. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 46. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 47. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 48. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 49. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 50. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 51. Musi posiadać możliwość eksportu danych użytkownika 52. Musi umożliwiać import listy urządzeń z pliku CSV 53. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 54. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 55. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; 56. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 57. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 58. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 59. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 60. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: 61. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 62. Portal musi być dostępny w postaci usługi hostowanej; 63. Skanowanie podatności za pomocą nodów skanujących 64. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 65. Portal zarządzający musi umożliwiać: 66. przegląd wybranych danych na podstawie konfigurowalnych widgetów 67. zablokowanie możliwości zmiany widgetów 68. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. 69. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności 70. eksport wszystkich skanów podatności do pliku CSV; |
| Oprogramowanie biurowe | Zainstalowane oprogramowanie biurowe- kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Wymagania odnośnie interfejsu użytkownika: 2. Pełna polska wersja językowa interfejsu użytkownika; 3. Prostota i intuicyjność obsługi, pozwalająca na prace osobom   nieposiadającym umiejętności technicznych;   1. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się; 2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki: 3. posiada kompletny i publicznie dostępny opis formatu, 4. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) 5. umożliwia wykorzystanie schematów XML 6. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766) 7. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców; 8. Zamawiający wymaga licencji przeznaczonych wyłącznie dla jednostek edukacyjnych; 9. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami; 10. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;. 11. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 12. Edytor tekstów 13. Arkusz kalkulacyjny 14. Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji 15. Narzędzie do zarzadzania informacja prywata (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) 16. Edytor tekstu musi umożliwiać: 17. Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty 18. Wstawianie oraz formatowanie tabel 19. Wstawianie oraz formatowanie obiektów graficznych 20. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne) 21. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków 22. Automatyczne tworzenie spisów treści 23. Formatowanie nagłówków i stopek stron 24. Sprawdzanie pisowni w języku polskim 25. Śledzenie zmian wprowadzonych przez użytkowników 26. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności 27. Określenie układu strony (pionowa/pozioma) 28. Wydruk dokumentów 29. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną 30. Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu 31. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 32. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem. 33. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. 34. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych. 35. Arkusz kalkulacyjny musi umożliwiać: 36. Tworzenie raportów tabelarycznych 37. Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych 38. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. 39. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) 40. Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych 41. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych 42. Wyszukiwanie i zamianę danych 43. Wykonywanie analiz danych przy użyciu formatowania warunkowego 44. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie 45. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności 46. Formatowanie czasu, daty i wartości finansowych z polskim formatem 47. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. 48. Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.. 49. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji 50. Narzędzie do projektowania i pracy z lokalnymi bazami danych, tego samego producenta, co reszta programów zawartych w oprogramowaniu biurowym; 51. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz: 52. Prezentowanie przy użyciu projektora multimedialnego 53. Drukowanie w formacie umożliwiającym robienie notatek 54. Zapisanie w postaci tylko do odczytu. 55. Nagrywanie narracji dołączanej do prezentacji 56. Opatrywanie slajdów notatkami dla prezentera 57. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo 58. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego 59. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym 60. Tworzenie animacji obiektów i całych slajdów 61. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera 62. Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016. 63. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać: 64. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego 65. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców 66. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną 67. Automatyczne grupowanie poczty o tym samym tytule 68. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy 69. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia 70. Zarzadzanie kalendarzem 71. Udostępnianie kalendarza innym użytkownikom 72. Przeglądanie kalendarza innych użytkowników 73. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach 74. Zarzadzanie lista zadań 75. Zlecanie zadań innym użytkownikom 76. Zarzadzanie listą kontaktów 77. Udostępnianie listy kontaktów innym użytkownikom 78. Przeglądanie listy kontaktów innych użytkowników 79. Możliwość przesyłania kontaktów innym użytkowników |
| Monitor | Rozmiar 23,8 cala;  Typ panelu VA  Podświetlenie W-LED  Powłoka ekranu Przeciwodblaskowa, 3H;  Format obrazu 16:9  Rozdzielczość 1920 x 1080  Czas reakcji matrycy Maksymalnie 5 ms.  Jasność 250  cd/m²  Kontrast 3000:1  Rozmiar plamki Maksymalnie 0,28 x 0,28 mm;   * Katy widzenia 178 stopni;   Złącza VGA, HDMI, wyjście audio,  Głośniki wbudowane 2 x 2W;  Pochylenie -5 do 20 stopni;  Pobór mocy Maksymalnie 15W;  Warunki gwarancji 3 lata;  Wymagania dodatkowe Blokada kansington, zgodnośc ze standardem VESA,  kabel HDMI; |

1. **Urządzenie wielofunkcyjne - 1 szt.;**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Technologia | Laser, mono |
| Funkcje | Kopiowanie, drukowanie, skanowanie; |
| Prędkośc drukowania | 30 str./min. |
| Obciążenie miesięcznie | 30 00 stron; |
| Procesor | 600 MHz; |
| RAM | 256 MB; |
| Złacza | Ethernet 10/100 Base TX;  USB 2.0;  WLAN 802.11.b/g/n |
| Czas wydruku/skopiowania pierwszej strony | Maksymalnie 10/15 s. |
| Rozdzielczośc wydruku/kopii | 1200/600 x 600 dpi; |
| Rozdzielczość skanowania | 1200 x 1200 dpi; |
| Formaty zeskanowanych plików | JPG, PDF, TIFF; |
| Podajnik/ odbiornik papieru | 250/100 arkuszy; |
| Bezpieczeństwo | Wyłączanie portów USB, IP Filtering, IP Sec; |
| Waga | Maksymalnie 12 kg |
| Wymagania dodatkowe | Skanowanie do poczty e-mail, FTP, USB, ADF, ekran LCD, wkład drukujący o pojemności 1500 wydruków; |
| **Gwarancja** | 24 miesiące; |

1. **Biurko komputerowe – 15 szt.;**
2. Stół jednoosobowy L regulowany w zakresach nr 2-5 lub 3-6
3. Przeznaczony do szkół ponadpodstawowych;
4. Metalowy stelaż o grubości min. 40 x 25mm malowany farbą proszkową;
5. Końcówki rur zabezpieczone stopkami z tworzywa;
6. Kolor blatu – buk;
7. Płyta o grubości min. 18 mm;
8. Okleina PCV o grubości min. 2 mm;
9. Wymiary blatu – min. 700 x 500mm
10. Musi posiadać  posiadać Certyfikat dopuszczający do użytku w placówkach oświatowych;
11. Gwarancja – 24 miesiące.
12. **Biurko nauczyciela - 1 szt.**
13. Dwuszafkkowe z 5 szufaladami w 2 kolumnach i zamykaną na klucz szafką z półką;
14. Szuflady zamykne centralnym zamkiem;
15. Wykonane z płyty laminowanej o grubości min. 18 mm;
16. Okleina PCV o grubości min. 2 mm;
17. Wymiary blatu – min. 1300 x 550 mm
18. Wysokość – min. 750 mm
19. Montaż;
20. Gwarancja – 24 miesiące.
21. **Tablica suchościeralna – 1 szt.;**

## Magnetyczna wykonana z blachy malowanej na biało;

## Powierzchnia tablicy musi pozwalać na używanie markerów ścieralnych oraz wszelkiego rodzaju magnesów

## Rozmiar - 150x100 cm;

## Aluminiowa rama;

## **Możliwość montowania w pionie oraz w poziomie**

## **Zestaw montażowy, półka na akcesoria, gąbka, zestaw 10 kolorowych magnesów oraz 4 kolorowych markerów;**

1. Gwarancja – 24 miesiące.
2. **Projektor multimedialny – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Jasność | 3800 lumenów |
| Rozdzielczość | 1280 x 800;; |
| Współczynnik proporcji | 4:3, 16:9, 16:10; |
| Kontrast | 30 000: 1 |
| Technologia wyświetlania | DLP |
| Moc lampy | 200W; |
| Żywotność lampy | 15 000h; |
| Zoom cyfrowy/optyczny | 2,0/1,1x |
| Odległośc rzutu | 1 – 10 m.; |
| Korekcja trapezu | +-40 stopni |
| Rozmiar obrazu | 0,7 – 7,5 m. |
| Współczynnik rzutu | 1,55:1 – 1,7:1 |
| Złącza | 2 x Jack 3,5 mm., 1 x HDMI 1,4, S-Video, 1 x USB, 1 x VGA; |
| Pobór mocy | Maksymalnie 270W; |
| Głośność | Maksymalnie 30 dB; |
| Waga | Maksymalnie 3 kg. |
| Warunki gwarancji | 2 lata na urządzenia, 1 rok na lampę; |
| Wymagania dodatkowe | Pilot, slot kensington Lock, blokada kodem PIN, timer, głośnik, tryby 2D i 3D, automatyczny wyłącznik, funkcja zamrożenia obrazu, komplet okablowania; |

1. **Pracownia komputerowa - serwer z oprogramowaniem – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ | Komputer stacjonarny. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Wydajność | Oferowany komputer przenośny musi osiągać w teście wydajności SYSMARK 2018 Overall rating, wynik 1850 pkt.  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 |
| Procesor | Musi osiągać wynik 23 800 w teście PassMark Average CPU Mark. |
| Pamięć operacyjna | 32GB DDR4 2400MHz, możliwość rozbudowy do 64GB, minimum 2 sloty wolne na dalszą rozbudowę.  Obsługa pamięci OC DDR4-4400 MHz. |
| Parametry pamięci masowej | 512GB SSD |
| Grafika | Ze wsparciem dla DirectX 11, ShaderModel 5.0, OpenGL 3.2 |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, 2 kanałowa; |
| Obudowa | Obudowa o sumie wymiarów nie większej niż 100cm.  Możliwość montażu beznarzędziowego dysku 3,5" oraz 2,5”, napędu optycznego i kart rozszerzeń. Obudowa wykonana z wytrzymałego tworzywa, blachy o grubości co najmniej 0,5 mm.  Możliwość montażu dysku 2,5" oraz 3,5" wewnątrz obudowy  Zatoki na dyski i napędy: 4× 2,5", 2× 2,5/3,5", 1× 3,5, 2 x 5,25”.  Wyposażona w 2 porty 3.1 z przodu obudowy  Wbudowana karta sieciowa 10/100/1000  Możliwość otwierania bez użycia narzędzi (wkręty ręczne)  Wyposażona w Kensington Lock i ucho na kłódkę  Zasilacz o mocy minimum 500W;  Zamontowane trzy fabrycznie filtry przeciwkurzowe, umiejscowione na froncie, pod zasilaczem oraz na topie obudowy.  Obudowa wyposażona w trzystopniowy kontroler obrotów na w sumie 6 wentylatorów |
| Certyfikaty i standardy | Komputer musi być wyprodukowany zgodnie z normami ISO 9001, ISO 27001, ISO 28000. |
| BIOS | 1. BIOS zgodny ze specyfikacją UEFI 2. Możliwość obsługi klawiaturą oraz myszą 3. Możliwość, bez uruchamiania systemu operacyjnego odczytania z BIOS informacji o: 4. wersji BIOS, 5. nr seryjnym serwera, 6. ilości pamięci RAM, 7. typie procesora, 8. pojemności zainstalowanego dysku twardego 9. rodzajach napędów optycznych 10. kontrolerze audio 11. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego 12. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń |
| Wymagania dodatkowe | 1. Wbudowane porty: 2. 1 x DisplayPort, 3. 1 x HDMI ver. 1.4 4. 8 portów USB wyprowadzonych na zewnątrz komputera w tym 2 porty USB 3.1 z przodu obudowy, 4szt. USB 3.1 z tyłu obudowy oraz 1szt. USB Type-C. Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp. 5. porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. 6. Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n 7. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL, PXE 2.1. 8. Płyta główna zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości., przeznaczona dla danego urządzenia; wyposażona w : 9. SATA III (6 Gb/s) - 6 szt. 10. M.2 - 3 szt. 11. PCIe 3.0 x16 - 2 szt. 12. PCIe 3.0 x1 - 4 szt. 13. 4 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, z obsługą DDR4-4400 MHz 14. Klawiatura USB w układzie polski programisty 15. Mysz USB z klawiszami oraz rolką (scroll) 16. Wbudowana w obudowę nagrywarka DVD +/-RW szybkość x24 wraz z oprogramowaniem do nagrywania i odtwarzania płyt 17. Wsparcie dla konfiguracji RAID 18. Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera. 19. System zasilania chroniący obwód specjalnie zaprojektowany przez producenta płyty głównej z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo złych zasilaczy. |
| System operacyjny | Musi spełniać następujące wymagana:   1. Licencja na 16 rdzeni procesorowych; 2. Wbudowany hypervisor wirtualizacyjny; 3. Możliwość stworzenia i używania 2 maszyn wirtualnych; 4. Licencje dostępowe dla 16 komputerów zamawiającego; 5. Analizator najlepszych praktyk; 6. Pamięć dynamiczna przy wirtualizacji; 7. Dodawanie i wymiana kości RAM bez wylączania systemu operacyjnego; 8. Konsola zarządzająca; 9. Sieciowy load balancing; 10. Migracja pamięci masowej; 11. Aktywacja zbiorcza; 12. Manager zasobów systemu operacyjnego; 13. Logowanie licencji serwera; 14. Nieograniczona liczba połączen RRAS; 15. Obsługa 64 gniazd 64 bitowych; 16. Obsługa 24 TB pamięci RAM; 17. Możliwość dołączenia do domeny; 18. Kodeki DLNA i strumieniowe przesyłanie multimediów internetowych; 19. Certyfikaty usług katalogowych; 20. Zarządzanie usługami katalogowymi; 21. Serwer: DHCP, DNS, iPAM, iSNS, SMTP, faksów, plików, dla NFS; 22. BranchCache dla plików sieciowych; 23. Deduplikacja danych; 24. Replikacja systemu plików DFS; 25. Funkcja serwera docelowego iSCSI I kontrolera sieci; 26. Mozliwośc dostępu i pulpitu zdalnego; 27. Usługi IIS; 28. Usługa inteligentnego transferu w tle; 29. Szyfrowanie I odblokowywanie dysków bitlocker; 30. Możliwość pracy w klastrze; 31. Zarządzanie politykami grupowymi; 32. Monitorowanie portów LPR; 33. Kolejkowanie wiadomości; 34. Protokół rozpoznawania nazw równorzędnych; 35. Manager połączeń RAS; 36. Zdaklna pomoc użytkownikom sieciowym; 37. Zdalna kompresja różnicowa; 38. RSAT; 39. RPC przez proxy HTTP; 40. Usługi TCP/IP; 41. Udostępnianie plików SMB 1.0/CIFS; 42. Klient Telnet i TFTP; 43. Wewnętrzna baza danych; 44. Kopia zapasowa serwera; 45. Narzędzia do migracji system operacyjnego; 46. Filtr TIFF IF; 47. Przeglądarka XPS; 48. Licencja bezterminowa; |
| Oprogramowanie zabezpieczające i diagnostyczne | 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, 2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, 3. Stosowanie kwarantanny; 4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) 5. Skanowanie urządzeń USB natychmiast po podłączeniu, 6. Automatyczne odłączanie zainfekowanej końcówki od sieci 7. 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. 8. 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. 9. Musi posiadać moduł ochrony IDS/IPS 10. Musi posiadać mechanizm wykrywania skanowania portów 11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów 12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości 13. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; 27. Konsola zarządzająca musi umożliwiać co najmniej: 28. przechowywanie danych w bazie typu SQL; 29. zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; 30. tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; 31. centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. 32. raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; 33. definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 34. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych   zainstalowanych w różnych lokalizacjach;   1. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 2. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 3. Musi posiadać dostęp do konsoli z dowolnego miejsca; 4. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 5. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 6. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych; 7. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 8. Konsola systemu musi umożliwiać, co najmniej: 9. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie 10. przyznanie praw dostępu dla nośników pamięci tj. USB, CD 11. regulowanie połączeń WiFi i Bluetooth 12. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe 13. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi 14. blokowanie dostępu dowolnemu urządzeniu 15. tymczasowe dodania dostępu do urządzenia przez administratora 16. szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; 17. zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka 18. zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora 19. używanie tylko zaufanych urządzeń sieciowych; 20. Wirtualna klawiatury 21. Możliwość blokowania każdej aplikacji 22. Możliwość zablokowania aplikacji w oparciu o kategorie 23. Możliwość dodania własnych aplikacji do listy zablokowanych 24. Dodawanie aplikacji w formie portable 25. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 26. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 27. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 28. Możliwość zablokowania funkcji Printscreen 29. Monitorowania przesyłu danych między aplikacjami; 30. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 31. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 32. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 33. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 34. Ochrona zawartości schowka systemu 35. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 36. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 37. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 38. Możliwość tworzenia profilu DLP dla każdej polityki 39. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 40. Ochrona przez wyciekiem plików poprzez programy typu p2p 41. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 42. Monitorowanie określonych rodzajów plików. 43. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 44. Możliwość śledzenia zmian we wszystkich plikach 45. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 46. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 47. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 48. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 49. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 50. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 51. Musi posiadać możliwość eksportu danych użytkownika 52. Musi umożliwiać import listy urządzeń z pliku CSV 53. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 54. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 55. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; 56. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 57. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 58. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 59. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 60. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: 61. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 62. Portal musi być dostępny w postaci usługi hostowanej; 63. Skanowanie podatności za pomocą nodów skanujących 64. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 65. Portal zarządzający musi umożliwiać: 66. przegląd wybranych danych na podstawie konfigurowalnych widgetów 67. zablokowanie możliwości zmiany widgetów 68. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. 69. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności 70. eksport wszystkich skanów podatności do pliku CSV;   Oprogramowanie producenta serwera umożliwiające zdalną i lokalną administrację oraz ich diagnostykę, pozwalające na:   * zdalną i lokalną inwentaryzację komponentów serwera * zdalne i lokalne monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS * zdalne włączenie, wyłączanie oraz restart serwera w sieci, * monitorowanie i alertowanie temperatur, napięć i zajętości dysków twardych wraz z wykresami; * Interfejs komunikacyjny w języku polskim; * w celu zapewnienia pełnej kompatybilności ww. oprogramowania z serwerem, musi być ono wyprodukowane w całości przez producenta serwera; |

1. **Kabel FTP kat. 6 - 200m.– 1 szt.**
2. Zgodność z dyrektywą CPR;
3. Klasa CPR - Dca s2 d2 a1;
4. Musi spełniać wymagania normy europejskiej EN 50575 w zakresie właściwości w warunkach działania ognia, metody badań i oceny kabli jako materiałów budowlanych;
5. Deklaracja właściwości użytkowych;
6. Skrętka ekranowana kategorii 6;
7. Musi być przeznaczona do wykonywania instalacji wewnątrz budynków;
8. Znacznik metrowy,
9. Ekran musi być wykonany z folii aluminiowej;
10. Żyły jednodrutowe miedziane o średnicy min. Ø0,5 mm;
11. Izolacja żył wykonana z HDPE;
12. Powłoka kabla musi być wykonana z polietylenu LSZH;
13. Musi być wyprodukowany zgodnie z normami: PN-EN-50173, EN 50173, ISO/IEC 61156-5/2002, ISO/IEC 11801;
14. Impedancja – 100Ω;
15. Prędkość propagacji NVP – 65%;
16. Rezystancja DC – 9 Ω/100m;
17. Promień gięcia – 8 x średnica kabla;
18. Gwarancja – 15 lat.
19. **Gniazda sieciowe RJ45 kat. 6 – 17 szt.**
20. **Puszka:**
21. Rozmiar – 35/50 mm.;
22. Montaż – zatrzsaki na szynie TT;
23. Zgodność z dyrektywą RoHS;
24. Materiał – polipropylen;
25. **Support;**
26. System – M45;
27. Montaż – natynkowy I podtynkowy;
28. Palność – V1 – V0;
29. Zgodność z dyrektywą RoHS;
30. Materiał – PVC-U;
31. **Ramka modułowa 1M;**
32. System – M45;
33. Montaż – natynkowy I podtynkowy;
34. Palność – V1 – V0;
35. Zgodność z dyrektywą RoHS;
36. Materiał – PVC-U;
37. **Adapter do gniazd RJ;**
38. System – 0,5 M45;
39. Montaż – natynkowy I podtynkowy;
40. Zgodność z dyrektywą RoHS;
41. Materiał – PVC-U;
42. **Moduł Keystone RJ-45 STP kat.6A;**
43. Musi być przeznaczony do budowy ekranowanych gniazd abonenckich oraz punktów krosowych w instalacjach zgodnych z ANSI/TIA/EIA 568 kat.6A;
44. Uniwersalne mocowanie pozwalające na łatwy montaż zarówno w panelach krosowych, jak i w puszkach naściennych / podłogowych;
45. Kształt obudowy musi zapewniać minimalny rozplot kabla;
46. Złącza szczelinowe muszą posiadać kolorowe kodowanie ułatwiające prawidłową instalację okablowania w sekwencjach;
47. Montaż modułu za pomocą dedykowanego narzędzia uderzeniowego;
48. Osłona zatrzaskowa zakładana na złącza szczelinowe;
49. kategoria 6A;
50. Metalowa obudowa;
51. Typ złącza szczelinowego - dual IDC;
52. Schemat połaczeń - EIA/TIA 568B i EIA/TIA 568A;
53. Gwarancja – 3 lata;
54. **Końcówki RJ45 – 100 szt.**
55. Złącze męskie 8P8C (RJ-45);
56. Kategoria 6;
57. Przeznaczona dozakańczania przewodów okrągłych (drutów) w instalacjach komputerowych;
58. Musi posiadać przelot na poszczególne żyły dla szybszego zarobienie złącza;
59. Złącze musi być wyposażone w sprężystą zapadkę zapobiegającą samoczynnemu wysuwaniu się z gniazda;
60. Gwarancja – 3 lata.
61. **Listwy montażowe - 30mb;**
62. Rozmiar 25x40x2000 mm – 20 mb;
63. Materiał – PVC-U;
64. Wyposazenie – pokrywa +kanał;
65. Palność – V1-V0;
66. Dekklaracja CE;
67. Certyfikat SEP-BBJ;
68. Rozmiar 60x110x2000 mm – 10 mb;
69. Materiał – PVC-U;
70. Wyposazenie – pokrywa +kanał+4 klamry;
71. Palność – V1-V0;
72. Dekklaracja CE;
73. Certyfikat SEP-BBJ.
74. **Switch – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Obsługiwane standardy | IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 802.3ab |
| Porty | 24 x 10/100/1000 Mb RJ45 |
| Obsługiwane kategorie okablowania | Od cat.3 UTP; |
| Prędkość portów | 148 8000 pps |
| Zabezpieczenie przeciwprzepięciowe | 6kV dla wszystkich portów |
| Prędkośc przełączania | 48 Gbps; |
| Rozmiar tabeli MAC adresów | 8 tys. |
| Kontrola dostępu | CDMA/CD |
| Pobór prądu | Maksymalnie 10 W; |
| Wymagania dodatkowe | Diody LED dla aktywnych portów |
| Gwarancja | 36 miesięcy; |

1. **Krosownica (patchpanel) 24 portowa z szafką rack– 1 kpl.**
2. Szafka rack:
3. Wysokość - 6U
4. Głębokość - 450 mm
5. Szerokość - 570 mm
6. Nośność - 60 kg
7. Otwór na przewody - w tylnej ścianie, od góry, od dołu
8. Otwory wentylacyjne - w ścianach bocznych, w drzwiach.
9. Zdejmowane ściany boczne,
10. Zdejmowana pokrywa w tylnej ścianie,
11. Możliwość montażu drzwi jako lewych bądź prawych,
12. Drzwi przednie zamykane na klamkę z zamkiem,
13. Ściany boczne zamykane na zamek,
14. W zestawie sześć kluczyków,
15. Cztery szyny RACK do montażu urządzeń;
16. Możliwość zmiany rozstawu między szynami przednimi a tylnymi.
17. Numerowane odstępy (1U) na listwach montażowych ,
18. Złącze uziemiające,
19. Możliwość montażu dwóch wentylatorów;,
20. Mocowanie na ścianie z wykorzystaniem uchwytu do mocowania szafy lub haków;.
21. Szafa musi być przeznaczona do montażu urządzeń z obudową w standardzie 19";
22. Gwarancja – 5 lat;
23. Listwa zasilająca do szafki rack;
24. Wysokość - 1U,
25. Mocowanie doczołowe do szyn rackowych,
26. Sygnalizacja zasilania na listwie za pomocą diody LED;
27. Prąd 16A (230 V AC),
28. Ilość gniazd - 9,
29. Kolor: czarny,
30. Długość przewodu - 150 cm,
31. Zestaw czterech śrub oraz koszyczków do montażu;
32. Gwarancja – 3 lata;
33. Patch panel do szafki rack;
34. Urządzenie ma stanowić zakończenie okablowania strukturalnego dla kabli sieciowych;
35. Panel musi umożliwić montaż modułów w standardzie Keystone do szafy RACK;
36. Wysokość - 1U
37. 24 porty
38. Mocowanie doczołowe do szyn rackowych
39. Kolor: Czarny
40. Gwarancja – 5 lat;
41. Poziomy organizer kabli do szafki rack;
42. Materiał – blacha stalowa
43. Wysokość - 1U
44. Mocowanie doczołowe do szyn rackowych
45. Kolor: Czarny
46. Gwarancja – 5 lat;
47. Patchcord – 17 szt.;
48. Rpdzaj – UTP;
49. Kategoria – 6;
50. Długość - 0,5 m’;
51. Średnica drutu przewodu - 0.5 mm.;
52. Powłoka kabla - polwinit PCV;
53. Wtyki RJ-45,
54. Gwarancja – 3 lata;
55. **Usługa (prace montażowe i instalacyjne):**
56. Przygotowanie sali komputerowej do instalacji.
57. Demontaż obecnej infrastruktury sieciowej.
58. Montaż koryt kablowych
59. Montaż okablowania strukturalnego LAN
60. Montaż szafy rack wiszącej
61. Montaż modułów keystone
62. Montaż gniazd LAN
63. Montaż akcesoriów wiszącej szafy „rack”
64. Testy okablowania
65. Opis obwodów LAN
66. Sprzątanie