*Załącznik nr 1 – Opis Przedmiotu Zamówienia*

**OPIS PRZEDMIOTU ZAMÓWIENIA – Część I Pomoce TIK**

1. **Mikroskop z podłączeniem do komputera**

|  |  |
| --- | --- |
| Mikroskop z podłączeniem do komputera – 3 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Mikroskop cyfrowy | Tak |
| Powiększenie w zakresie 20–230x | Tak |
| Kamera cyfrowa 2 Mpx | Tak |
| Robienie zdjęć i nagrywanie filmów z przebiegu obserwacji | Tak |
| System oświetlenia | 8 białych diod LED z regulowaną jasnością |
| W zestawie: | Statyw  Osłona soczewki obiektywowej wykonana z tworzywa sztucznego  Oprogramowanie do przetwarzania obrazu  Instrukcja obsługi i karta gwarancyjna |
| Gwarancja | Min. 2 lata |

1. **Mikroskop z kamerą USB**

|  |
| --- |
| Mikroskop z kamerą USB – 3 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Mikroskop ze szklaną optyką, zakresem powiększeń 40x-400x | tak |
| Stolik mechaniczny, z możliwością precyzyjnego przesuwu preparatu, z naniesioną podziałką | tak |
| Oświetlenie LED: górnym (odbitym) i dolnym (przechodzącym) | tak |
| Cyfrowa kolorowa kamera mikroskopowa | tak |
| Maksymalna rozdzielczość: 1600 x 1200 pikseli (2 megapiksele) | tak |
| Rozmiar sensora (przekątna): 4.73x3.52mm (1/3.2") | tak |
| Wielkość piksela: 2.8 µm x 2.8 µm | tak |
| Zakres dynamiki: 71 dB | tak |
| Przetwornik analogowo-cyfrowy: 8-bit R.G.B | tak |
| Interfejs: USB 2.0 | tak |
| Kabel USB do połączenia z komputerem | tak |
| Gwarancja | 2 lata |

1. **Aparat fotograficzny**

|  |
| --- |
| Aparat fotograficzny – 3 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Rozdzielczość | Min 16 Mpix |
| Zbliżenie optyczne | Min 40 x |
| Ogniskowa (dla 35 mm) | 22,5 - 900 mm |
| [Stabilizator obrazu](https://www.euro.com.pl/slownik.bhtml?definitionId=14251744961) optyczny + cyfrowy | tak |
| Dodatkowa karta SD | Min 32 GB |
| Torba do aparatu | tak |
| Gwarancja | 12 miesięcy |

1. **Rzutnik multimedialny**

|  |
| --- |
| Rzutnik multimedialny– 3 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Technologia | 3LCD |
| Rozdzielczość | Min. 1024 x 768 (XGA) |
| Podstawowy format obrazu | 4:3 |
| Jasność | Min. 3300 ANSI Lumenów |
| Kontrast | Min. 20000:1 |
| Trwałość lampy | Min. 6000 h (tryb normalny)  Min. 12500 h (tryb Eko) |
| Moc lampy | Min. 280 W UHP |
| Automatyczne zmniejszenie mocy lampy (zmniejszenie jasności) po zadanym czasie jeżeli nie zmienia się wyświetlany obraz | TAK |
| Automatyczne dopasowanie mocy lampy do jasności wyświetlanego obrazu | TAK |
| Stosunek odległości do szerokości obrazu | odległość projekcyjna przy szerokości wyświetlanego obrazu 250 cm–w zakresie od 372 do 447 cm |
| Głośnik | 1W Mono |
| Wejście audio | 1 x para RCA, 2 x 3,5mm stereo |
| Wyjście audio | 1 x 3,5mm stereo |
| Wejście cyfrowe | 1 x HDMI (zgodny z HDCP) |
| Wejście komputerowe analogowe | 2 x 15-pin Mini D-sub (współdzielone z wyjściem monitora) |
| Wyjście komputerowe analogowe | 1 x 15-pin Mini D-sub (współdzielone z wejściem komputerowym) |
| RS-232C | Tak |
| Poziom hałasu | Max. 37dB (tryb Normal)/ 29dB (Tryb Eco) |
| Korekcja efektu trapezowego | W pionie: manualna ±30 stopni (@XGA 60Hz) |
| Obiektyw | Ręczna regulacja Zoom 1.2 Ręczna regulacja ostrości |
| Wymiary - suma | 650 - 800 mm |
| Waga | Max. 3.6 kg |
| Dostarczone wyposażenie | Pilot zdalnego sterowania z bateriami , kabel RGB, kabel zasilający, instrukcja obsługi (szczegółowa i skrócona), uchwyt sufitowy |
| Gwarancja producenta na projektor i lampę | 36 miesięcy |

|  |  |
| --- | --- |
| Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta oraz musi być realizowany zgodnie z normą ISO 9001– wymagane oświadczenie **Wykonawcy** potwierdzające, że serwis będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta oraz, że będzie realizowany zgodnie z normą ISO 9001 | Tak (należy dołączyć do oferty oświadczenie **Wykonawcy** lub na dalszym etapie postępowania) |
| Certyfikat ISO 9001 dla producenta lub równoważne potwierdzające spełnienie przez producenta sprzętu norm w zakresie wymogów koniecznych do spełnienia dla uzyskania wskazanych certyfikatów ISO | Tak ~~(dołączyć do oferty odpowiedni dokument potwierdzający, że sprzęt jest produkowany zgodnie ze wskazaną normą )~~ |
| Deklaracja CE | Tak ~~(dołączyć do oferty )~~ |

1. **Ekran do rzutnika**

|  |
| --- |
| Ekran do rzutnika multimedialnego/projektora – 3 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Przekątna | 215 - 220 cm |
| Wymiary | 170 - 185 x 130 - 140 cm |
| Powierzchnia zwiększająca kontrast oglądanego obrazu | tak |
| Regulacja wysokości ekranu oraz dolnej krawędzi | tak |
| Składany trójnóg z gumowymi końcówkami zapewniającymi stabilność | tak |
| Gwarancja | 12 miesięcy |

1. **Laptop/ Przenośny komputer dla ucznia wraz z oprogramowaniem/** **Przenośny komputer dla nauczyciela wraz z oprogramowaniem**

|  |  |
| --- | --- |
| Laptop/ Przenośny komputer dla ucznia wraz z oprogramowaniem/ Przenośny komputer dla nauczyciela wraz z oprogramowaniem – 29 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
|  | |
| Ekran | TFT 15.6” LED TFT Full-HD o rozdzielczości min. 1920x1080 (16:9), z powłoką matową, nie dopuszcza się matryc typu "glare", wyposażony w technologię zmniejszającą ilość odbijanego światła na ekranie. Klapa komputera otwierana do 180 stopni. |
| Wydajność/ Procesor | Procesor uzyskujący wynik co najmniej 5000 punktów w teście Passmark - CPU Mark według wyników procesorów publikowanych na stronie http://www.cpubenchmark.net/cpu\_list.php (na dzień nie wcześniejszy niż 01.09.2019). W ofercie wymagane podanie producenta i modelu procesora. ~~Do oferty należy załączyć wydruk ze strony potwierdzający ww. wynik.~~ |
| Chipset | Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora. |
| Obudowa | Dopuszczalne kolory - czarny, srebrny, grafitowy, szary lub ich kombinacje.  Umożliwiająca bezpośredni dostęp do dysków HDD, SSD oraz pamięci RAM, bez konieczności odkręcania całej dolnej pokrywy notebooka. ~~Spełniająca normę MIL-STD 810G + (odporność na upadek z wysokości 122cm oraz zachlapanie)~~ |
| Pamięć RAM | Min. 16GB DDR4 (pamięć RAM rozszerzalna do 24GB) |
| Dysk twardy | Min. 1x 256GB SSD |
| Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:  - systemu operacyjnego  ~~- oprogramowania antywirusowego~~  Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania. |
| Napęd optyczny | 8x DVD +/- RW Super Multi Dual Layer wewnętrzny lub równoważny (parametry porównywalne, nie gorsze) |
| Karta graficzna | Karta grafiki z dedykowaną pamięcią 2GB ze wspraciem dla OpenGL 4.5, OpenCL 1.2, Microsoft DirectX 12. Powinna osiągać w teście wydajności: PassMarkPerformanceTest wynik min. 2100 punktów w G3D Mark (wynik dostępny: http://www.videocardbenchmark.net/gpu\_list.php) (na dzień nie wcześniejszy niż 01.09.2019). |
| Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki 2W stereo oraz cyfrowy mikrofon |
| Połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LAN (WOL Ready)  WLAN 802.11 ac/b/g/n/ac supports Intel® Wi-Di wraz z Bluetooth 4.2 lub równoważny (parametry porównywalne, nie gorsze) |
| Porty/złącza  (wbudowane) | 1 x Złącze RJ-45 (podłączenie sieci lokalnej)  1 x Czytnik Kart pamięci SD™  2 x USB 2.0  2 x USB 3.1 (w tym 1xType-C Gen.1 )  1 x VGA  1 x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)  1 x HDMI ze wsparciem HDCP  1 x zasilanie DC-in |
| Klawiatura | Pełnowymiarowa z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura musi być wyposażona w 2 klawisze ALT (prawy i lewy).  Klawiatura typu CHICLET. |
| Urządzenie wskazujące | Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka posiadającą certyfikat Microsoft Precision Touchpad Certification. |
| Kamera | Wbudowana, o parametrach:  - HD 1280 x 720 rozdzielczość minimalna  - min. 720p HD audio/video nagrywanie |
| Bateria | ~~Litowo-jonowa 3 komorowa 51,5 Wh 4515 mAh – czas pracy min. 14h według karty katalogowej producenta.~~  Litowo-jonowa, oferująca czas pracy komputera co najmniej 8 godzin według producenta. |
| Zasilacz | Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 65W. |
| Bezpieczeństwo | - Zabezpieczenie BIOS hasłem użytkownika.  - Zabezpieczenie dysku twardego hasłem użytkownika.  - Złącze typu Kensington Lock.  - Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego - Trusted Platform Module 2.0. |
| Gwarancja | a) Gwarancja producenta komputera min 36 miesięcy –  b) Gwarancja na baterię min. 12 miesięcy.  c) Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta  d) Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera.  e) Wymagane okno czasowe dla zgłaszania usterek min wszystkie dni robocze w godzinach od 8:00 do 17:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne. |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. 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.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN  e. Certyfikat/Klucz i uwierzytelnienie biometryczne  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |
| Oprogramowanie dodatkowe | A) Oprogramowanie pozwalające na:  - Szyfrowanie i deszyfrowanie pojedyńczych plików i folderów  - Zamazywanie plików z dysku twardego zgodne z certyfikatem DoD 5220.22M  - Osobisty strzeżony dysk (PSD) w postaci bezpiecznej partycji, w którym można przechowywać poufne pliki. Dostęp do plików zapisanych w formacie PSD można uzyskać tylko po wprowadzeniu uwierzytelniającego hasła.  - Ustawienia BIOS: ustawienie sekwencji bootowania, ustawienie haseł dostępu, Import/Export ustawień, blokowanie portów i urządzeń.  B) Oprogramowanie służące do zarządzania komputerami w sieci, pozwalające minimum na:  - Zarządzanie regułami  - Szeregowanie i alarmy  - Zarządzanie zapasami  - Kwerendy i raporty  - Generowanie raportu środków trwałych (z możliwością eksportu danych do pliku xls.)  raz w tygodniu bez konieczności dokonywania spisu lokalnie lub zdalnie.  Wygenerowany raport musi zawierać:  a) numer seryjny komputera,  b) informacje o zainstalowanym dysku HDD,  c) informacje o zainstalowanym systemie,  d) informacje o zainstalowanym procesorze,  e) informacje o zainstalowanej pamięci operacyjnej RAM,  Do oferty należy dołączyć oświadczenie **Wykonawcy (ogólne oświadczenie)**, że oferowane oprogramowanie jest w pełni kompatybilne z oferowanym sprzętem.  W ofercie można podać nazwę oferowanego oprogramowania dodatkowego. |
| Certyfikaty i standardy | Certyfikat ISO 9001:2000 dla producenta sprzętu.  Certyfikat ISO 14001 dla producenta sprzętu.  Oferowany model notebooka musi posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanego modelu notebooka z systemem operacyjnym Windows 10.  Deklaracja zgodności CE |
| Wsparcie techniczne producenta | A) Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – ~~do oferty należy dołączyć link strony.~~  B) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera.  C) W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji.  D) ~~Do oferty należy dołączyć kartę katalogową/specyfikację techniczą urządzenia. Karta powinna zawierać wyraźne zdjęcia obudowy oferowanego komputera~~. |

1. **Lodówka z zamrażalnikiem**

|  |
| --- |
| Lodówka z zamrażalnikiem – 3 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Wymiary | (WxSxG) między 120 x 45 x 60 a 150 x 60 x 70 |
| Pojemność chłodziarki/zamrażarki | Ok. 130/40 l |
| Położenie zamrażarki | Na górze |
| Zmiana kierunku otwierania drzwi | Tak |
| Klasa energetyczna | A+ |
| [Pojemność użytkowa chłodziarki](https://www.euro.com.pl/slownik.bhtml?definitionId=363527732) | Ok. 120 l |
| [Pojemność użytkowa zamrażarki](https://www.euro.com.pl/slownik.bhtml?definitionId=363529142) | Ok. 35 l |
| Gwarancja | 24 miesiące |

1. **Oprogramowanie biurowe**

|  |  |
| --- | --- |
| Oprogramowanie biurowe – 26 licencji | |
| Opis minimalnych wymaganych parametrów sprzętu | |
|  | |
| Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej | tak |
| Wymagania odnośnie interfejsu użytkownika | a. Pełna polska wersja językowa interfejsu użytkownika. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. |
| Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie | Parametry formatu: a. posiada kompletny i publicznie dostępny opis formatu, b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526), c. Pozwala zapisywać dokumenty w formacie XML. |
| Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji. | tak |
| W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). | tak |
| Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. | tak |
| Aplikacje wchodzące w skład pakietu | a. Edytor tekstów  b. Arkusz kalkulacyjny  c. Narzędzie do przygotowywania i prowadzenia prezentacji d. Narzędzie do tworzenia drukowanych materiałów informacyjnych e. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) f. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR. |

|  |  |
| --- | --- |
| Funkcje edytora tekstów | |
| Edycja i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. | tak |
| Wstawianie oraz formatowanie tabel. | tak |
| Wstawianie oraz formatowanie obiektów graficznych. | tak |
| Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). | tak |
| Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. | tak |
| Automatyczne tworzenie spisów treści. | tak |
| Formatowanie nagłówków i stopek stron. | tak |
| Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. | tak |
| Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. | tak |
| Określenie układu strony (pionowa/pozioma). | tak |
| Wydruk dokumentów. | tak |
| Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. | tak |
| Praca na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. | tak |
| Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. | tak |
| Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem. | tak |
| 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. | tak |
| Funkcje arkusza kalkulacyjnego | |
| Tworzenie raportów tabelarycznych | tak |
| Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych | tak |
| Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. | tak |
| Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) | tak |
| Obsługa kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych | tak |
| Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych | tak |
| Wyszukiwanie i zamianę danych | tak |
| Wykonywanie analiz danych przy użyciu formatowania warunkowego | tak |
| Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie | tak |
| Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności | tak |
| Formatowanie czasu, daty i wartości finansowych z polskim formatem | tak |
| Zapis wielu arkuszy kalkulacyjnych w jednym pliku. | tak |
| Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. | tak |
| Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. | tak |
| Funkcje narzędzia do przygotowywania i prowadzenia prezentacji |  |
| Przygotowywanie prezentacji multimedialnych, które będą: b. Prezentowanie przy użyciu projektora multimedialnego c. Drukowanie w formacie umożliwiającym robienie notatek d. Zapisanie jako prezentacja tylko do odczytu. e. Nagrywanie narracji i dołączanie jej do prezentacji f. Opatrywanie slajdów notatkami dla prezentera g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym j. Możliwość tworzenia animacji obiektów i całych slajdów k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010 i 2013. | tak |
| Funkcje narzędzia do tworzenia drukowanych materiałów informacyjnych | |
| Tworzenie i edycję drukowanych materiałów informacyjnych | tak |
| Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów. | tak |
| Edycja poszczególnych stron materiałów. | tak |
| Podział treści na kolumny. | tak |
| Umieszczanie elementów graficznych. | tak |
| Wykorzystanie mechanizmu korespondencji seryjnej. | tak |
| Płynne przesuwanie elementów po całej stronie publikacji. | tak |
| Eksport publikacji do formatu PDF oraz TIFF. | tak |
| Wydruk publikacji. | tak |
| Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. | tak |
| Funkcje narzędzia do zarządzania informacją prywatną | |
| Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, | tak |
| Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, | tak |
| Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, | tak |
| Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, | tak |
| Automatyczne grupowanie poczty o tym samym tytule, | tak |
| Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, | tak |
| Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, | tak |
| Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, | tak |
| Zarządzanie kalendarzem, | tak |
| Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, | tak |
| Przeglądanie kalendarza innych użytkowników, | tak |
| Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, | tak |
| Zarządzanie listą zadań, | tak |
| Zlecanie zadań innym użytkownikom, | tak |
| Zarządzanie listą kontaktów, | tak |
| Udostępnianie listy kontaktów innym użytkownikom, | tak |
| Przeglądanie listy kontaktów innych użytkowników, | tak |
| Możliwość przesyłania kontaktów innym użytkowników, | tak |
| Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http. | tak |

1. **Oprogramowanie antywirusowe**

|  |
| --- |
| Oprogramowanie antywirusowe – 26 licencji |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
|  | |
| Pełne wsparcie dla systemu Windows: 10, 8.x, 7, Vista, Server 2016, Server  2012, Server 2008, 2003 Server. | tak |
| Wsparcie dla systemów XP SP3 32-bit, Linux 32/64-bit, OS X (tylko klient). | tak |
| Interfejsy programu, pomoce i podręczniki w języku polskim. | tak |
| Pomoc techniczna w języku polskim. | tak |
| Potwierdzona średnia skuteczność oprogramowania we wszystkich testach „File  Detection Test of Malicious Software” z roku 2012 i 2013 przeprowadzonych przez  organizację AV-Comparatives przynajmniej na poziomie 99,5% wykrytych  zagrożeń. | tak |
| 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.  2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware,  phishing, hacktools itp.  3. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i  nieaktywne rootkity.  4. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.  5. Klient oprogramowania antywirusowego dla linuksowych serwerów Samba.  6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych  plików.  7. 2 niezależne skanery antywirusowe (nie heurystyczne!) z 2 niezależnymi bazami  sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz  skaner poczty elektronicznej.  8. Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami  antywirusowymi jednocześnie.  9. Dodatkowy i niezależny od skanerów plików, trzeci skaner poczty oparty o  technologię cloud security.  10. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów,  plików lub procesów.  11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików  na żądanie lub według harmonogramu.  12. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu  (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie  może być uruchomione z innymi ustawieniami (metody skanowania, obiekty  skanowania, czynności, rodzaj plików do skanowania, priorytet skanowania).  13. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w  menu kontekstowym.  14. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy  czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4  tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.  15. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie  i według harmonogramu.  16. Możliwość skanowania dysków sieciowych i dysków przenośnych.  17. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.  18. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych  przez skaner dostępowy.  19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny  obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być  przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.  20. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym,  zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji  roboczej (niezależnie od konkretnego klienta pocztowego).  21. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez  konieczności zmian w konfiguracji.  22. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma  odbywać się skanowanie.  23. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej  odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.  24. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z  ochroną z poziomu programu pocztowego.  25. Dodatek do aplikacji MS Outlook umożliwia ponowne skanowanie wszystkich  nieprzeczytanych wiadomość znajdujących się w skrzynce  26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest  automatycznie blokowany a użytkownikowi wyświetlane jest stosowne  powiadomienie.  27. Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z  bankami i sklepami online.  28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności  zmian w konfiguracji.  29. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się  skanowanie.  30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do  laboratorium producenta.  31. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek  nowych zagrożeń powinny być w pełni anonimowe.  32. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do  dowolnej stacji roboczej w sieci lokalnej.  33. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do  użytkownika i/lub administratora poprzez e mail.  34. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.  35. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego  zewnętrznie.  36. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.  37. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.  38. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np.  komputery mobilne).  39. Program wyposażony w tylko w jeden serwer skanujący uruchamiany w pamięci,  z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody  heurystyczne, skaner HTTP).  40. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.  41. Kontrola zachowania aplikacji (Behaviour Blocking) do wykrywania podejrzanie  zachowujących się aplikacji.  42. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz  na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on  używany.  43. Ochrona przed urządzeniami podszywającymi się po klawiatury USB.  44. Moduł do ochrony przed exploitami (ataki 0-day). | tak |
| Zdalne administrowanie ochroną |
| 1. Integracja z Active Directory – import kont komputerów i jednostek  organizacyjnych.  2. Ochrona dla urządzeń z systemem Android.  3. Zarządzanie urządzeniami z systemem iOS.  4. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich  podłączonych komputerach Active Directory.  5. Zdalna instalacja i centralne zarządzanie klientami na stacjach roboczych i  serwerach Windows.  6. Zdalna instalacja i centralne zarządzanie klientami Linux / OS X.  7. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent.  Na końcówkach zainstalowany jest sam program antywirusowy.  8. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli  (przynajmniej aktualizacje, ochronę przeglądarek, skanowania zasobów,  synchronizacji raportów).  9. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.  10. Możliwość eksportu/importu ustawień dla stacji/grupy stacji.  11. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna  konsoli.  12. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta  z jednego okna konsoli.  13. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer  główny i serwery podrzędne).  14. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego  automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia  serwera głównego.  15. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy  połączenia VPN.  16. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez  przeglądarki internetowe (z sieci lokalnej i spoza niej).  17. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez  urządzenia mobilne (smartfony, tablety) oparte o system Android (z sieci lokalnej i  spoza niej).  18. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.  19. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.  20. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji  roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników  skanowania).  21. Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach  (nazwa, wersja, producent, data instalacji).  22. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie  w poszukiwaniu stacji je posiadających.  23. Odczyt informacji o zasobach sprzętowych stacji (procesor i jego taktowanie, ilość  pamięci RAM i ilość miejsca na dysku/partycji systemowej).  24. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.  25. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu  niezabezpieczonych stacji roboczych.  26. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy  wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.  27. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli  zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są  zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające  ustawienia konfiguracyjne).  28. Możliwość generowania raportów w formacie XML.  29. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub  wykresów.  30. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji  roboczej lub grupie stacji roboczych.  31. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji  roboczej.  32. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości  jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji  roboczych.  33. Możliwość dynamicznego grupowania stacji na podstawie parametrów: nazwa  komputera, adres IP, brama domyślna, nazwa domeny. | tak |
| Raporty |
| 1. Możliwość utworzenia raportów statusu ochrony sieci.  2. Możliwość generowania raportów w przynajmniej 3 językach.  3. Możliwość wysyłania raportów z określonym interwałem.  4. Możliwość wysłania jednego raportu na różne adresy mailowe lub grupy adresów.  5. Możliwość zdefiniowania przynajmniej 15 różnych typów informacji dotyczących  statusu ochrony oraz różnych form ich przedstawienia (tabele, wykresy) w  pojedynczym raporcie. | tak |
| Licencja na 3 lata | tak |

1. **Wózek na laptopy**

|  |
| --- |
| Wózek na laptopy – 2 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Wózek na kółkach | tak |
| Możliwa ilość przechowywanych urządzeń | Min 26 |
| Możliwość ładowania baterii do laptopów/tabletów | tak |
| Wewnętrzna listwa zasilająca z gniazdem elektrycznym | tak |
| Ilość kolumn | Min 2 |
| Ilość gniazdek | Min 13 |
| Drzwi wózka zabezpieczone zamkiem kluczowym | tak |
| Waga | Max 95 kg |
| Deklaracje zgodności z Dyr. Parlamentu Europejskiego Dyrektywa niskonapięciowa LVD2014/35/UE D. U.2016 | Tak |
| Farba - Klasyfikacje ogniowa wg EN 13501, Atest Higieniczny PZH | tak |
| Gwarancja | 24 miesiące |

1. **Klimatyzator**

|  |
| --- |
| Klimatyzator – 2 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| 4 tryby pracy (chłodzenie, ogrzewanie, osuszenie, cyrkulacja) | Tak |
| 24-godzinny timer | Tak |
| Tryb turbo chłodzenie | Tak |
| Zmywalne filtr powietrza | Tak |
| Klasa energetyczna A/A+ | Tak |
| Ekologiczny czynnik R410A | Tak |
| Elektroniczna regulacja temperatury | Tak |
| Automatyczne odprowadzanie skroplin w trybie chłodzenia | Tak |
| SWING - regulacja kierunku nawiewu | Tak |
| Pilot zdalnego sterowania w zestawie | Tak |
| 3-stopniowa regulacja prędkości wentylatora oraz tryb AUTO | Tak |
| Wyposażenie | - rura odprowadzająca ciepłe powietrze,  - końcówka wlotu rury,  - końcówka wylotu rury,  - wężyk odpływowy,  - pilot zdalnego sterowania + baterie (2 x AAA),  - osłona na okno przesuwne,  - instrukcja obsługi |
| Gwarancja | 36 miesięcy |

1. **Router**

|  |  |
| --- | --- |
| Router – 2 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Porty | WAN 1: 1 x VDSL / ADSL (RJ11) WAN 2: 1 x 1Gb WAN 3-4: USB (Modem 4G, drukarka, NAS) |
| Switch | 4 x 1Gb z funkcją VLAN tagging 802.1Q |
| Firewall | - **Filtr danych** - blokowanie lub przepuszczanie ruchu w/g założonych kryteriów - **Kontrola Aplikacji**- blokowanie ruchu P2P,  aplikacji IM, protokołów, oraz oprogramowania odpowiedzialnego za tunelowanie, strumieniowanie i zdalną kontrolę  **- Filtr zawartości URL** - blokowanie  lub przepuszczanie  na podstawie fraz adresów URL. Możliwość stworzenia profili dla grup użytkowników  - **Filtr treści Web -** blokowanie lub przepuszczanie stron internetowych w/g kategorii (np. sex, czat, haking), biała/czarna lista. Możliwość stworzenia profili dla grup użytkowników  **- Filtr DNS** - blokowanie lub przepuszczanie ruchu na podstawie analizy zapytań DNS |
| Zarządzanie pasmem | **- Bandwith Limit** (tryby: każdy, dzielony) - limitowanie pasma pozwalające definiować maksymalny upload i maksymalny download  **- Limit Sesion** - limitowania sesji NAT pozwalające definiować maksymalną liczbę nawiązanych sesji |
| VPN | **- serwer/klient** VPN dla połączeń typu **LAN-LAN** (łączenie zdalnych sieci LAN) oraz serwer VPN dla połączeń typu **Host-LAN** (zdalny dostęp pojedynczych stacji)  - Możliwość stworzenia 30 jednoczesnych tuneli z wykorzystaniem protokołów:  IPSec - zabezpieczenia AH lub ESP (szyfrowanie DES, 3DES, AES) z funkcjami haszującymi MD5 lub SHA1. Uwierzytelnianie IKE odbywa się przy pomocy klucza PSK lub podpisu cyfrowego (X.509).  PPTP - szyfrowanie MPPE 40/128 bitów oraz uwierzytelnianie PAP, CHAP, MS-CHAPv1/2.  L2TP  - uwierzytelnianie PAP, CHAP, MS-CHAPv1/2.  L2TP over IPSec - tunel L2TP zabezpieczony IPSec.  - Możliwość stowrzenia 10 tuneli VPN SSL |
| Obsługa mechanizmu **VPN trunk** wraz **VPN Load-balance** i **VPN Backup** | Tak |
| Centralne zarządzanie | - centralne zarządzanie Access Pointami  WLAN Profile - 5 profili ustawień sieci bezprzewodowej które można zastosować do wybranych AP  AP Maintenance - backup/przywracanie konfiguracji, aktualizacja firmware  AP Traffic Graph - wykresy ruchu AP  Rogue AP Detection - wykrywanie podejrzanych AP  AP Load Balance - rozkład obciążenia pomiedzy AP  - centralne zarządzanie routerami wspierającymi VPN |
| WLAN | wbudowany Access Point w standardzie IEEE 802.11ac, pracujący w pasmach 2,4GHz i 5GHz.  możliwość stworzenia niezależnych 4 podsieci bezprzewodowych  obsługa min. 64 użytkowników  możliwe tryby pracy: bridge, repeater  możliwość instalacji anten zewnętrznych poprzez złącza RP-SMA. |
| Funkcje dodatkowe | obsługa protokołu IPv6  NAT, Multi-NAT  hosty DMZ, przekierowania portów, otwarte porty dla podsieci na cele NAT dla ruchu przychodzącego, dokonywane niezależnie dla różnych adresów publicznych  podsieci LAN: LAN1 (NAT), LAN2 - LAN4 (NAT lub routing), Routing  protokoły routingu: trasy statyczne, RIPv2  obsługa dynamicznego DNS  wake on LAN (wystarczy się zalogować na router i wybrać komputer w sieci, który chcemy obudzić)  serwer DHCP i DNS Proxy  synchronizacja czasu przez Internet (klient NTP)  standard UPnP (kontrola stanu połączenia WAN, automatyczne otwieranie portów na żądanie aplikacji)  reguły czasowe dla wybranych funkcji (dostęp do Internetu, mechanizmy firewall) |
| Gwarancja | 24 miesiące |

1. **Kontroler WLAN**

|  |  |
| --- | --- |
| Kontroler WLAN – 2 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Procesor | Min. czterordzeniowy |
| Pamięć | Min. 1GB |
| Port | 1 x 1Gb |
| Zasilanie | PoE 48V 802.af lub Passive PoE,  MicroUSB 5V 1A |
| Ilość obsługiwanych Access Pointów | 20 |
| Licencja pozwalająca zarządzać min. 20 Access Pointami | Tak |
| Zarządzanie za pomocą WWW | Tak |
| Możliwość zarządzania urządzeniami znajdującymi się w kilku lokalizacjach | Tak |
| Funkcje zarządzania | - monitorowanie i mapowanie urządzeń  - szczegółowa analiza jakości sygnału  - obsługa portalu dla gości |
| Możliwość zarządzania urządzeniami: | - router  - przełącznik |
| Możliwość konfiguracji sieci | WAN/LAN/VLAN |
| Możliwość monitorowania i analizowania wydajności każdego portu w przełączniku | Tak |
| Możliwość konfiguracji grup użytkowników | TAK |
| Wyposażenie dodatkowe | Kabel krosowy, zasilacz POE lub MicroUSB |
| Gwarancja | 24 miesiące |

1. **Bezprzewodowe punkty dostępowe**

|  |  |
| --- | --- |
| Bezprzewodowe punkty dostępowe – 6 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Port LAN | 1 x 1Gb |
| Wbudowany przycisk RESET | TAk |
| Wbudowana dioda Status LED | Tak |
| Obsługiwane standardy sieci WiFi | 802.11 a/b/g/n/ac |
| Antena | Dwu-zakresowa, 3-polaryzacyjna |
| Pasmo | 2,4GHz i 5GHz |
| Moc nadawania 2,4GHz | 24dBm |
| Moc nadawania 5GHz | 22dBm |
| Szyfrowanie | TKIP - Temporal Key Integrity Protocol  AES - standard szyfrowania danych  WEP - Wired Equivalent Privacy  WPA - Enterprise  WPA (PSK) - Wi-Fi Protected Access (Pre-Shared Keys) WPA2 - Wi-Fi Protected Access II |
| Obsługa SSID | Po 4 na każde pasmo |
| Montaż | Ścienny lub sufitowy  Wymagane dostarczenie odpowiednich uchytów montażowych |
| Zasilanie | PoE lub Passive PoE (wymagane dostarczenie odpowiedniego zasilacza) |
| Gwarancja | 24 miesiące |

1. **Serwer plików NAS**

|  |  |
| --- | --- |
| Serwer plików NAS – 2 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Procesor | Dwurdzeniowy, o częstotliwości 1,2GHz |
| Wbudowana pamięć | Min. 512MB |
| Zatoki | 2 x 3,5” lub 2,5” SATA z obsługą dysków SSD i HDD |
| Porty zewnętrzne | 2 x USB 3.0, 1 x RJ45 |
| Typ obudowy | Tower |
| Macierze RAID | RAID 0, RAID 1 |
| System plików | ext4, ext3, FAT, NTFS |
| Zarządzanie pamięcią masową | Liczba wewnętrznych wolumenów: 64  Liczba iSCSI Target: 10  Liczba jednostek iSCSI LUN: 10 |
| Obsługiwane protokoły sieciowe | SMB1-3, NFS, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP |
| Funkcja udostępniania plików | Liczba kont użytkowników lokalnych: 1024  Licza grup lokalnych: 256  Liczba flderów współdzielonych: 256 |
| Zainstalowane dyski | 2 x 1TB SATA, dedykowane do pracy w urządzeniach typu NAS |
| Zasilanie | 230V |
| Wymiary | Suma wymiarów nie większa niż: 600mm |
| Wyposażenie | Kabel sieciowy UTP  Instrukcja obsługi  Zasilacz |
| Gwarancja | 24 miesiące |

1. **Oprogramowanie do zarządzania pracownią**

|  |  |
| --- | --- |
| Oprogramowanie do zarządzania pracownią – 26 licencji | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Oprogramowanie do zarządzania mobilną pracownią komputerową | Oprogramowanie musi być w polskiej wersji językowej i musi posiadać wsparcie producenta komputera, pozwalające minimum na:  - podglądanie ekranów na komputerach uczniowskich  - przesyłanie ekranów z komputera nauczyciela na komputery uczniowskie  - blokowanie klawiatury, myszy, ekranu na komputerach uczniowskich  - archiwizowanie ekranów i innych materiałów do późniejszego wykorzystania  - monitorowanie dostępu do Internetu  - tworzenie testów: rozsyłanie pytań i gromadzenie odpowiedzi; tworzenie zestawu pytań  - współpraca z tablicą interaktywną  - monitoring i archiwizacja plików audio. |
| Licencja bezterminowa | Tak |

1. **Sieciowe urządzenie wielofunkcyjne**

|  |
| --- |
| Sieciowe urządzenie wielofunkcyjne – 1 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Technologia druku | technologia laserowa |
| Funkcje standardowe | kopiarka, drukarka sieciowa, kolorowy skaner sieciowy |
| Format oryginału | A4 |
| Format kopii | A4-A6 |
| Prędkość druku | Min. 40 stron A4 / min. |
| Dostępne rozdzielczości drukowania | min. 600x600 dpi i 1200 x 1200 dpi |
| Czas wydruku pierwszej strony | maks. 7 sek. |
| Czas nagrzewania | maks. 20 sek. |
| Kopiowanie wielokrotne | 1- 999 kopii |
| Pamięć RAM | min. 512 MB (możliwość rozbudowy do min. 1536 MB) |
| Zoom | 25-400% |
| Panel operatora | wyposażony w ekran LCD,  opisy na panelu oraz komunikaty na ekranie w języku polskim |
| Dupleks | automatyczny, w standardzie |
| Podajnik dokumentów | automatyczny, dwustronny - jednoprzebiegowy, na min. 50 ark. (80 g/m2), w standardzie |
| Podajniki papieru | min. 1 kaseta na min. 250 ark. A5-A4 (80 g/m2), 60-160 g/m2;  taca uniwersalna na min. 50 ark. A6-A4 (80 g/m2), 60-220 g/m2 |
| Funkcja druku sieciowego | w standardzie |
| Emulacje | PCL 6, PostScript 3 |
| Interfejsy | USB 2.0, Ethernet 10/100/1000Base-T, USB dla pamięci przenośnej, gniazdo karty SD |
| Funkcja skanowania sieciowego | w standardzie, skanowanie pełno-kolorowe |
| Funkcje skanowania | skanowanie do e-mail, do FTP, do-SMB, TWAIN, WSD, do pamięci przenośnej USB, skanowanie ciągłe |
| Rozdzielczość skanowania | 600 dpi |
| Prędkość skanowania | W trybie mono: min. 40 obrazów/min. (A4, 300 dpi),  W trybie kolorowym: min. 20 obrazów/ min. (A4, 300 dpi) |
| Typy plików | PDF, JPEG, TIFF, XPS |
| Możliwość rozbudowy | Dodatkowy podajnik lub podajniki papieru, o pojemności łącznej min. 500 ark. formatu A4 – A5, 80 g/m2 |
| Materiały eksploatacyjne jako wyposażenie standardowe  (dostarczone w komplecie w ramach oferowanej ceny jednostkowej). | Tonery - właściwa ilość, która zapewni wydrukowanie minimum 3 000 stron A4 przy pokryciu zgodnie z ISO19752.  Bębny - właściwa ilość, która zapewni wydrukowanie minimum 100 000 stron A4. Dostarczone materiały muszą być nowe i nieużywane, pierwszej kategorii oraz wyprodukowane przez producenta oferowanych urządzeń. |
| Gwarancja | 24 miesiące |

1. **Aparat fotograficzny**

|  |
| --- |
| Aparat fotograficzny – 1 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |  |
| --- | --- |
| Rozdzielczość | Min 16 Mpix |
| Zbliżenie optyczne | Min 40 x |
| Ogniskowa (dla 35 mm) | 22,5 - 900 mm |
| [Stabilizator obrazu](https://www.euro.com.pl/slownik.bhtml?definitionId=14251744961) optyczny + cyfrowy | tak |
| Dodatkowa karta SD | Min 32 GB |
| Torba do aparatu | tak |
| Gwarancja | 1. miesięcy |

1. **Zasilacz UPS**

|  |  |
| --- | --- |
| Zasilacz UPS – 2 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Moc pozorna | 1000VA |
| Moc rzeczywista | 600W |
| Zakres napięcia wejściowego | 190-250 V |
| Zakres częstotliwości wejściowej | 45 – 55 Hz |
| Zakres napięcia wyjściowego | 230 V |
| Częstotliwość napięcia wyjściowego | 50 Hz |
| Czas przełączenia na pracę rezerwową | Max. 7ms |
| Czas podtrzymania przy obciążeniu 100% | 4min |
| Czas podtrzymania przy obciążeniu 50% | 6min |
| Gniazda wyjściowe z podtrzymaniem | 4 x IEC 320 C13 (10 A) |
| Gniazda wyjściowe bez podtrzymania | 4 x IEC 320 C13 (10 A) |
| Interfejsy komunikacyjne | USB |
| Oprogramowanie monitorująco-zarządzające | Tak |
| Zimny Start | Tak |
| Sygnalizacja | Akustyczno-optyczna |
| Wyświetlacz LCD | Tak |
| Gwarancja producenta | 24 miesiące |

1. **Elementy sieci – instalacja i integracja**

|  |  |
| --- | --- |
| Elementy sieci – instalacja i integracja – 1 usługa | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Instalacja i integracja dostarczonych elementów sieci | tak |

1. **Zestaw interaktywny**

|  |
| --- |
| Zestaw interaktywny – 1 szt. |
| Opis minimalnych wymaganych parametrów sprzętu |

|  |
| --- |
| **Tablica** |

|  |  |
| --- | --- |
| Panel / rozdzielczość | Min. 32768 x 32768 |
| Przekątna | 84" |
| Model | DTO-i78C |
| Obszar interaktywny [szer. / wys.] | 145,00 – 160,00 cm x 110,00 – 120,00 cm |
| Proporcje obrazu / format | 4:3 |
| Przekątna obszaru interaktywnego | Ok. 200 cm (78") |
| Wymiar zew. [szer. / wys.] | Max. 1670 cm x 1260 cm |
| Przekątna wymiaru zew. | Ok. 2110 cm (83,6") |
| Typ powierzchni tablicy | ceramiczna, matowa, magnetyczna powierzchnia, 25 lat gwarancji na powierzchnię |
| Dodatkowe cechy tablicy | - suchościeralna o wysokiej odporności  na zarysowania i uszkodzenia mechaniczne;   - antyodblaskowa matowa powierzchnia;  - łatwa w czyszczeniu;  - technologia rozpoznawania gestów multi-gesture;  - dostosowana do używania pisaków suchościeralnych; |
| Technologia dotyku | podczerwień (IR) |
| Ilość obsługiwanych punktów dotyku | 10 TOUCH - jednoczesna praca dziesięciu osób bez konieczności dzielenia obszaru roboczego na 10 stref |
| Rejestracja dotyku | pisak, palce lub inne nieprzezroczyste obiekty |
| Prędkość kursora / tempo śledzenia | 6 ms - 12 ms |
| Czułość na dotyk | odbiór dotyku i zbliżenia pisaka mniej niż 2 mm od powierzchni tablicy |
| Obsługiwany system operacyjny | Windows: 10, 8.1, 8,7, Vista, XP / Linux / Mac |
| Oprogramowanie | tak |
| funkcja udostępniania ekranu | tak |
| Przydatne funkcje | rozpoznawanie pisma odręcznego, odtwarzanie wideo z możliwością „pisania” na filmie, zrzuty wideo, szybkie tworzenie figur geometrycznych, bogata biblioteka załączników związanych z przedmiotami szkolnymi, współpraca z większością formatów graficznych, integracja z programami MS Office pozwalająca na ręczne dopisywanie notatek do dokumentów (w formie graficznej) |
|  |  |
| Waga | Max. 23 kg |
| Grubość | Max. 4 cm |
| Funkcja myszy | tak |
| Technologia Plug & Play | tak |
| Zasilanie | USB / DC 4.6V - 5.0V <1W |
| Zużycie energii | < 250 mA |
| Certyfikaty | CE, ROHS, ISO 9001, ISO 14001 |
| Gwarancja | 5 lat na tablicę, 1 rok na pozostałe komponenty |
| Dołączone  akcesoria | Półka na pisaki, kabel USB, 2 pisaki, gąbka, oprogramowanie na płycie CD, zestaw montażowy |

|  |  |
| --- | --- |
| **Głośnik** | |
| Moc RMS | 3 Wat |
| Ilość głośników | 2 szt. |
| Wyjście audio (słuchawkowe) | 1 x mini jack 3,5mm |
| Wejście audio | 1 x mini jack 3,5mm |
| Regulacja głośności | Pokrętło na jednym z głośników wraz z funkcją ON/OFF |
| Gwarancja | 24 miesiące |
| **Projektor** | |

|  |  |
| --- | --- |
| Technologia 3LCD | tak |
| Rozdzielczość | Min. 1024 x 768 (XGA) |
| Format 4:3 | tak |
| Jasność | min. 3100 ANSI Lumenów |
| Kontrast | min. 10 000:1 |
| Żywotność lampy | Min. 5000 h (tryb normalny), 8000 h (tryb Eko1) 10000 h (tryb Eko2) |
| Moc lampy | max. 330 W |
| Projektor musi umożliwić wyświetlenie obrazu o przekątnej 80 cali (format 4:3) z odległości nie większej niż 125 cm (odległość od obrazu do najbardziej oddalonego od niej elementu projektora) przy zachowaniu proporcji obrazu, jego formatu, a także zapewniając ostrość na całej powierzchni bez stosowania jakichkolwiek elektronicznych korekcji | tak |
| Głośnik | min. 16W Mono |
| Wejście audio | 1 x para RCA, 1 x 3,5mm stereo |
| Wyjście audio | 1 x 3,5mm stereo |
| Wejście cyfrowe | 2 x HDMI |
| Wejście komputerowe analogowe | 2 x 15-pin Mini D-sub (współdzielone z wyjściem monitora) |
| Wyjście komputerowe analogowe | 1 x 15-pin Mini D-sub (współdzielone z wejściem komputerowym) |
| Wejścia Video | 1 x RCA dla composite) |
| Port RS-232C | tak |
| Poziom hałasu | max. 36dB (tryb Normal)/32dB (Tryb Eco1)/29dB (Tryb Eco2) |
| Zabezpieczenia antykradzieżowe kodem PIN | tak |
| Wymiary | Suma wymiarów: max 800 mm |
| Waga | max. 3,6 kg |
| Wyposażenie Pilot zdalnego sterowania z bateriami , kabel RGB, kabel zasilający, instrukcja obsługi (szczegółowa i skrócona),kabel HDMI 10 m, dodatkowy kabel zasilający do projektora 10m | tak |
| Filtr powietrza, który użytkownik sam może wymienić i wyczyścić bez konieczności demontażu projektora i użycia narzędzi | tak |
| Wymiana lampy bez konieczności demontażu projektora | tak |
| Funkcja blokady klawiatury uniemożliwiająca osobom niepowołanym na samodzielne włączenie i obsługę projektora bez nadzoru | tak |
| Co najmniej 2 uchwyty do montażu mechanicznych zabezpieczeń przeciw kradzieżowych – przygotowane przez producenta projektora | tak |
| Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta oraz musi być realizowany zgodnie z normą ISO 9001– wymagane oświadczenie **Wykonawcy** potwierdzające, że serwis będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta oraz, że będzie realizowany zgodnie z normą ISO 9001 | Tak (należy dołączyć do oferty lub po otwarciu ofert ) |
| Deklaracja CE – ~~dołączyć do oferty~~ | Tak |
| Gwarancja producenta na projektor i lampę 36 miesięcy | tak |
| **Uchwyt do projektora** | |
| Uchwyt mocujący do ściany | minimalne płynne regulacje: odległość od ściany bliżej/dalej, pochylenie projektora przód/tył, pochylenie na prawo/lewo, odchylenie od ściany prawo/lewo, prowadzenie kabli – wewnątrz konstrukcji uchwytu |

|  |  |
| --- | --- |
| **Instalacja projektora ( okablowanie, zasilanie )** | |
| Projektor musi być zainstalowany na uchwycie ściennym. | tak |
| Wszystkie przewody niezbędne do prawidłowego funkcjonowania projektora o długości min. 15 m Wykonawca musi poprowadzić w listwach instalacyjnych do miejsca, w którym zaplanowane zostało umieszczenie komputera przenośnego. Przewody sygnałowe (HDMI ) i zasilania muszą być podłączone odpowiednio do projektora i tablicy interaktywnej z jednej strony, a komputerem z drugiej strony. | tak |

1. **Zintegrowana brama zabezpieczająca**

|  |  |
| --- | --- |
| Zintegrowana brama zabezpieczająca – 2 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN | tak |
| W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu | tak |
| System musi wspierać IPv4 oraz IPv6 w zakresie:  Firewall.  Ochrony w warstwie aplikacji.  Protokołów routingu dynamicznego. | tak |
| W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. | tak |
| Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. | tak |
| Monitoring stanu realizowanych połączeń VPN. | tak |
| System realizujący funkcję Firewall musi dysponować minimum 5 portami Gigabit Ethernet RJ-45. | tak |
| System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. | tak |
| W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. | tak |
| System musi być wyposażony w zasilanie AC. | tak |
| W zakresie Firewall’a obsługa nie mniej niż 900 tys. jednoczesnych połączeń oraz 15.000 nowych połączeń na sekundę. | tak |
| Przepustowość Stateful Firewall: nie mniej niż 0.95 Gbps. | tak |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 400 Mbps. | tak |
| Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 75 Mbps. | tak |
| Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 300 Mbps. | tak |
| Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 150 Mbps. | tak |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 120 Mbps. | tak |
| W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. | tak |
| Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. | tak |
| System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:   * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP. | tak |
| W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN | tak |
| 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site. | tak |
| 1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. | tak |
| 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego. * Policy Based Routingu. | tak |
| System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. | tak |
| System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | tak |
| Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. | tak |
| System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | tak |
| Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) | tak |
| System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. | tak |
| System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). | tak |
| Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. | tak |
| Ochrana przed atakami na aplikacje pracujące na niestandardowych portach. | tak |
| Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | tak |
| Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. | tak |
| System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. | tak |
| Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | tak |
| Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | tak |
| Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | tak |
| Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. | tak |
| Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. | tak |
| Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | tak |
| Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. | tak |
| W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. | tak |
| Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. | tak |
| Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. | tak |
| System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. | tak |
| Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. | tak |
| 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. | tak |
| Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. | tak |
| Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. | tak |
| Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. | tak |
| Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów | tak |
| Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. | tak |
| System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. | tak |
| System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall | tak |
| System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. | tak |
| W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania | tak |
| Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu | tak |
| Musi istnieć możliwość logowania do serwera SYSLOG. | tak |
| Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. * ICSA lub NSS Labs dla funkcji IPS. * ICSA dla funkcji IPSec VPN. * ICSA dla funkcji SSL VPN. | tak |
| W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. | tak |
| Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesiące, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5. | tak |
| ~~Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).~~ | ~~tak~~ |
| Certyfikat ISO 9001 podmiotu serwisującego. | tak |
| W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. | Tak (na żądanie Zamawiającego) |
| ~~Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.~~ | ~~tak~~ |

1. **Tablet**

|  |  |
| --- | --- |
| Tablet – 13 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Ekran | Przekątna min. 10.1”, rozdzielczość min. 1920 x 1200 w technologii IPS; 10-punktowy, TFT |
| Pamięć RAM | Min. 2 GB |
| Pamięć wbudowana | Min. 32 GB |
| Procesor | Ośmiordzeniowy, dedykowany do urządzeń mobilnych |
| Multimedia | Wbudowane głośniki stereo  Wbudowane dwa mikrofony  Radio FM  Aluminiowa obudowa  Aparat: 5.0 Mpix – przód; 8.0 Mpix - tył |
| Rozdzielczość nagrywania wideo | FullHD (1920 x 1080) |
| Bateria | Litowo-polimerowa min. 6000 mAh |
| Certyfikaty | Deklaracja zgodności CE lub równoważne |
| System operacyjny | System operacyjny przeznaczony do mobilnych urządzeń przenośnych obsługujących technologię dotykową |
| Porty i złącza, komunikacja. | USB Type-C - 1 szt.  Wyjście słuchawkowe - 1 szt.  Czytnik kart pamięci - 1 szt. |
| Warunki gwarancji | Gwarancja producenta min. 24 miesiące. |

1. **Zestaw do nauki programowania dla klas starszych**

|  |  |
| --- | --- |
| Zestaw do nauki programowania dla klas starszych – 12 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Zawartość zestawu | * Programowalna kostka * 3 interaktywne serwomotory (2 duże i jeden średni), * Czujnik dotyku, * Czujnik koloru, * Czujnik podczerwieni, * Pilot na podczerwień, * Zestaw kabli, * 594 klocków |
| Czujnik kolorów | Tak, odróżniający min 7 barw |
| **Zasilanie** | 6 [baterii AA](http://neorobot.pl/pl/zasilanie) |
| **System kompatybilne wstecz**, co oznacza, że przy budowaniu nowych robotów można korzystać ze wszystkich posiadanych już elementów tej serii | tak |
| Platforma zawierająca gotowe instrukcje budowania robotów | tak |
| Gwarancja | 24 miesiące |

**Tonery**

|  |  |
| --- | --- |
| Tonery – 23 szt. | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| **Poz. 25** Toner do Konica Minolta bizhub 163, czarny, wydajność min. 11 000 stron | 1 szt. |
| **Poz. 26** Toner do HP Ink Advantage 1515, toner czarny - wydajność 360 stron | 21 szt. |
| **Poz. 27** Toner do SharpMX-M316N/MX-M266N, 315 g, żywotność 27 500 kopii | 1 szt. |

1. **Papier do wydruków**

|  |  |
| --- | --- |
| Papier do wydruków – 72 szt. ( ryzy ) | |
| Opis minimalnych wymaganych parametrów sprzętu | |
| Ryza | 500 arkuszy |
| Gramatura | 80 g |