1 . Komputer stacjonarny wraz z oprogramowaniem - 96 szt

Parametr	Parametry wymagane
Obudowa	Typu „All-in-one" z wyświetlaczem LCD zintegrowanym w obudowie komputera (nie zezwala się rozwiązań modułowych gdzie monitor i komputer stanowią dwa oddzielne urządzenia) wyposażona w 2 wbudowane głośniki audio min 2x2W, w min. 1 gniazdo słuchawek i min. 1 gniazdo mikrofonu, w min. 2 gniazda USB szybkiego dostępu zlokalizowane bocznej części obudowy, oraz statyw umożliwiający ustawienie komputera na biurku. Wymiary bez podstawy max 340x545x65 (wys/szer/gł). Obudowa z plastiku ABS, przedni panel ze szkła hartowanego o podwyższonej wytrzymałości Obudowa umożliwiająca zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)
Wyświetlacz	Min. 21,5" LCD w technologii LED, o formacie obrazu 16:9, o minimalnej rozdzielczości w poziomie 1920 pikseli i o minimalnej rozdzielczości w pionie 1080 pikseli, zabezpieczony szybą
Procesor	Procesor klasy x86, min. dwurdzeniowy, umożliwiający osiągnięcie przez oferowany zestaw w teście **SYSmark® 2014 wyniku całkowitego Rating – 990 punktów**, Wymagane dołączenie wyniku testu przeprowadzonego na oferowanej konfiguracji i potwierdzającego osiągnięcie przez oferowany zestaw komputerowy wymaganego wyniku (wynik w postaci wydruku z programu Sysmark 2014 v 1.5)
Płyta główna	Chipset min H110 współpracujący z procesorami czterordzeniowymi wspierający pamięci DDR4 dedykowany dla procesora, Typ podstawki: dedykowany dla procesora 6 x USB w tym minimum 2 x USB 3.0 dostępne z zewnątrz komputera Minimum 2 x USB wyprowadzone na bok obudowy Min 2 x SATA III Min 1 x mSATA
BIOS	BIOS zgodny ze specyfikacją UEFI.
Audio	karta dźwiękowa zintegrowana, zgodna z HD audio, mikrofon wbudowany w obudowę komputera
Pamięć RAM	Min. 6GB DDR4 2133MHz z możliwością rozszerzenia do 32GB, min 1 wolny slot pamięci
Dysk twardy	Dysk twardy o pojemności 500 GB, z interfejsem przynajmniej SATA2, z buforem minimum 8MB, pracujący z prędkością obrotową 5400 obr./min
Napęd optyczny	Wbudowana nagrywarka DVD +/-RW wraz z oprogramowaniem
Karta grafiki	Zintegrowana z płytą główną, wolne zewnętrzne złącza: 1 x HDMI, 1 x DVI
Porty zewnętrzne	min. 1xHDMI, 1xDVI,, 1xAudio Line out, 1xMic, min. 4 x USB z tyłu obudowy (w tym min 2 x USB 3.0), 2 x USB 2.0 z boku obudowy
Komunikacja przewodowa	gigabit ethernet 10/100/1000 Mb/s ze złączem RJ 45, z obsługą WOL WiFi 802.11 b/g/n
Czytnik kart pamięci	Wbudowany, 4 in 1, zlokalizowany na boku obudowy
Kamera	zintegrowana z obudową ekranu minimum 1,3MP z mechaniczną przysłoną
Zasilacz	min. 150W, zewnętrzny, zgodny z Energy Star 5.0
Klawiatura	w układzie polski programisty, przewodowa
Mysz	Optyczna z dwoma klawiszami oraz rolką (scroll), przewodowa
System operacyjny	System operacyjny klasy desktop 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. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim, 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe, 4. Wbudowany system pomocy w języku polskim; 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, 9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, 16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, 17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, 18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 20. 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, 21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 22. Obsługa standardu NFC (near field communication), 23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 26. Mechanizmy logowania do domeny w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 27. Mechanizmy wieloelementowego uwierzytelniania. 28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5, 29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 30. Wsparcie dla algorytmów Suite B (RFC 4869),

	31. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, 32. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 34. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 35. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 36. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową, 37. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację, 38. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, 39. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 40. Udostępnianie modemu, 41. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, 42. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, 43. 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.), 44. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu), 45. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych, 46. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, 47. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 48. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych 49. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 50. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.System nie wymagający aktywacji (dopuszcza się licencję elektroniczną z kluczem licencyjnym zapisanym w BIOS)
Certyfikaty	- Certyfikat PN-EN ISO 9001:2001(ISO 9001:2001) na procesy projektowania, produkcję, sprzedaż i serwis, PN-EN ISO14001:2005 (ISO 14001:2005) oraz PN-ISO/IEC 27001:2007 lub nowsze - deklaracja producenta o zgodności z dyrektywami 73/23/EEC oraz 89/336/EEC (oznaczenia CE) - Deklaracja producenta sprzętu o zgodności oferowanego komputera z wymaganiami normy Energy Star 6.1. Wymagane potwierdzenie obecności oferowanego modelu na stronie internetowej Energy Star przez dostarczenie wydruku ze strony http://www.eu-energystar.org z kategorii Integrated Desktop Computers.
Gwarancja	3 lata gwarancji

	Serwis – Zamawiający wymaga aby serwis był realizowany przez producenta oferowanego sprzętu lub autoryzowanego partnera serwisowego producenta oferowanego sprzętu Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera (załączyć dokument potwierdzający spełnianie wymogu)
Sterowniki	Możliwość ściągnięcia aktualnych sterowników z witryny producenta komputera poprzez podanie numeru seryjnego komputera – załączyć zrzut witryny producenta komputera z niniejszą funkcjonalnością.
Oprogramowanie biurowe	Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej, 2. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika. b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: 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. 4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji. 5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 6. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. 7. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 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. 8. Edytor tekstów musi umożliwiać: a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. b. Wstawianie oraz formatowanie tabel.

	c. Wstawianie oraz formatowanie obiektów graficznych. d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. f. Automatyczne tworzenie spisów treści. g. Formatowanie nagłówków i stopek stron. h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. j. Określenie układu strony (pionowa/pozioma). k. Wydruk dokumentów. l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem. p. 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. 9. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych g. Wyszukiwanie i zamianę danych h. Wykonywanie analiz danych przy użyciu formatowania warunkowego

	i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności k. Formatowanie czasu, daty i wartości finansowych z polskim formatem l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. m. 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. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. 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. 11. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów. c. Edycję poszczególnych stron materiałów. d. Podział treści na kolumny. e. Umieszczanie elementów graficznych. f. Wykorzystanie mechanizmu korespondencji seryjnej. g. Płynne przesuwanie elementów po całej stronie publikacji. h. Eksport publikacji do formatu PDF oraz TIFF. i. Wydruk publikacji. j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 12. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,

	b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, e. Automatyczne grupowanie poczty o tym samym tytule, f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, i. Zarządzanie kalendarzem, j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, k. Przeglądanie kalendarza innych użytkowników, l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, m. Zarządzanie listą zadań, n. Zlecanie zadań innym użytkownikom, o. Zarządzanie listą kontaktów, p. Udostępnianie listy kontaktów innym użytkownikom, q. Przeglądanie listy kontaktów innych użytkowników, r. Możliwość przesyłania kontaktów innym użytkowników, s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
Oprogramowanie Antywirusowe	1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. 4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. 5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives **Ochrona antywirusowa i antyspyware** 6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 8. Wbudowana technologia do ochrony przed rootkitami. 9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 12. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało

	czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 14. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 15. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. 16. Możliwość skanowania dysków sieciowych i dysków przenośnych. 17. Skanowanie plików spakowanych i skompresowanych. 18. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 19. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 20. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 21. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 22. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 23. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 24. 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. 25. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). 26. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 27. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 28. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 29. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 31. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.

	32. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. 33. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 34. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 35. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 36. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 37. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 38. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 39. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 40. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 41. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. 42. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 43. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 44. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 45. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 46. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 47. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 48. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 49. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.

	50. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 51. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. 52. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 53. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 54. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 55. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 56. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu. 57. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 58. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. 59. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 60. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 61. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 62. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 63. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 64. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

	• tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach. • Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 65. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 66. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 67. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 68. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 69. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 70. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 71. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 72. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 73. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 74. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 75. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 76. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 77. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 78. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 79. Program ma być w pełni zgodny z technologią CISCO Network Access Control. 80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. 81. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.

	82. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. 83. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 85. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. 86. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 87. Możliwość podejrzenia licencji za pomocą, której program został aktywowany. Ochrona serwera plików Windows 1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016 SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. 2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami i exploitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 12. Możliwość skanowania dysków sieciowych i dysków przenośnych. 13. Skanowanie plików spakowanych i skompresowanych. 14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 16. Aplikacja powinna wspierać mechanizm klastrowania.

	17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire. 21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika. 23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. 24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 34. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 35. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 36. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. 37. Aktualizacje modułów analizy heurystycznej.

	38. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 39. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 40. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych. 41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 43. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 44. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 45. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. 46. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 47. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. 48. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. 49. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu. 50. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB. 54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych,

	informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 58. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 61. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu. 62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 63. Aplikacja musi wspierać skanowanie magazynu Hyper-V 64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 65. Praca programu musi być niezauważalna dla użytkownika. 66. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania. 67. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna** Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. 1. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 2. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 3. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. 4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 6. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.

	7. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 8. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 9. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. 10. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 11. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 12. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 13. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. 14. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 15. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 16. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym. 17. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 18. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. 19. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. 20. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 21. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 22. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. 23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. 24. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 25. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 26. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. 27. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej 28. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.

	29. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 30. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. 31. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny. 32. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 33. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. 34. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 35. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 36. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. 37. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 38. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej 39. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 40. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. 41. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 42. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 43. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 44. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. 45. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 46. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. 47. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.

	48. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 50. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji. 51. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 52. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. 53. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 54. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 55. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. 56. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. 57. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 58. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. 59. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. 60. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. 61. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 62. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 63. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora. 64. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta 65. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.

	66. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 67. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 68. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp. 69. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania. 70. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów. 71. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. 72. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 73. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 74. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. 75. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. 76. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 77. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 78. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. 79. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. 80. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 81. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 82. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 83. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 84. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.

	85. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 86. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. 87. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. 88. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 89. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).

2.) Kolorowa drukarka laserowa + skaner – 2szt

Parametr	**Opis**
Pojemność wejściowa	Podajnik 1: 300 arkuszy
Podajnik uniwersalny	100 arkuszy
Rozdzielczość skanowania	min 600 x 600 dpi
Rozdzielczość kopiowania	min 600 x 1200 dpi
Format oryginalny	A3, A4, A5, A6, B4, B5, Letter, Legal 13, Legal 13.5, Legal 14, Executive, Tabloid (11" x 17"), Statement, Folio, rozmiar niestandardowy
Format papieru do kopiowania	A3, A4, A5, A6, B4, B5, B6, Letter, Legal 13, Legal 13.5, Legal 14, Executive, Tabloid (11" x 17"), Statement, Folio, 8K, 16K, koperty,
Skalowanie kopiowania	min25-400%
Panel sterowania	Ekran dotykowy LCD 7-calowy (17,5cm) podświetlany kolorowy ekran dotykowy LCD i górne przyciski;
Szybkość kopiowania	min 23 kopii na minutę w formacie A4 w kolorze, 23 kopii na minutę w formacie A4 w czerni
Czas uzyskania pierwszej kopii	W kolorze: około 14,5 sekundy; w czerni: około 14,5 sekundy
Czas nagrzewania	Około 32,0 s od momentu włączenia
Zasilanie	220-240 V AC ±0%
Pobór mocy	Podczas pracy: max. 1 400W / Śr. 850W Tryb gotowości: max 120W
Pamięć (Std./Maks.)	min 1,2GB/1,2GB
Bezpieczeństwo i przepisy dotyczące środowiska	Blue Angel, Energy Star, Dyrektywa dotycząca kompatybilności elektromagnetycznej, Oznaczenie GS, Oznaczenie CE
Poziom hałasu	Podczas pracy: max 55 dBA
Podczas pracy	11-31°C, 21-79% wilgotność względna
Wymiary (wys. x szer. x głęb.)	max 564 x 601 x 701 mm
Waga (wraz z materiałami eksploatacyjnymi)	max 65,0 kg
Obciążalność max.	60 000 stron miesięcznie
DRUK Szybkość drukowania	min A4 23 str./min w kolorze, 23 str./min monochromatyczne A3 13 str./min w kolorze, 13 str./min monochromatyczne

Czas uzyskania pierwszej kopii	W kolorze: około 14,5 sekundy; w czerni: około 14,5 sekundy
Rozdzielczość druku	min 600 x 600 dpi 600 x 1200 dpi (4 poziomy)600 x 600 dpi
Fizyczna wielkość plamki	min 600 dpi
Interfejs	1000BASE-T/100BASE-TX/10BASE-T, USB 2.0 (High Speed), Host USB 2.0 (High Speed), Protokół
Język drukarki	Emulacja PostScript 3, emulacja PDF v1.7, emulacja PCL 5c, emulacja PCL 6 (XL), emulacja XPS, emulacja IBM ProPrinter, emulacja Epson FX
Obsługiwane systemy operacyjne	Windows 8.1, Windows 8.1 x64, Windows 8, Windows 8 x64, Windows 7, Windows 7 x64, Windows Vista, Windows Vista x64, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2008 x64, Windows Server 2003, Windows Server 2003 x64, Mac OS X 10.6, OS X 10.7, OS X 10.8, OS X 10.9, OS X 10.10,
Czcionka	Czcionki Adobe PostScript 80, 87 skalowalnych czcionek emulacji PCL, 4 czcionki bitmapowe
FAX Format papieru	min A3, A4, A5, A6, B4, B5, B6, Letter, Legal 13, Legal 13.5, Legal 14, Executive, Tabloid (11" x 17"), Statement, Folio, 8K, 16K, koperty, pocztówka, pocztówka zwrotna, rozmiar niestandardowy

3.) Serwer - 5szt

Parametr	**Opis**
Płyta główna	Serwerowa, jednoprocesorowa z możliwością instalacji modułu TPM
Procesor	Jeden procesor przynajmniej 4-rdzeniowy taktowany zegarem minimum 2,26 GHz posiadający pamięć podręczną cache o wielkości przynajmniej 8MB.
Zarządzanie	Zintegrowany moduł zarządzający z dedykowanym portem RJ45 i pełnym przekierowaniem konsoli KVM
Złącza kart rozszerzeń	Minimum 1x PCI-E 3.0 x8 (x16 slot), 1x PCI-E 3.0 x8 oraz 1x PCI-E 3.0 x4 (x8 slot)
Pamięć	Co najmniej 8GB RAM, możliwość rozbudowy do 64GB,
Karta sieciowa	Dwa porty 1Gb Ethernet (niezależne od karty zarządzającej), obsługa startu z iSCSI oraz PXE
Karta graficzna	Zintegrowana z płytą główną
Kontroler RAID	Zintegrowany z płytą główną kontroler SATA RAID 0,1,10, posiadający co najmniej sześć złącz SATA 6Gbps
Dysk twardy	Dwa dyski SSD przeznaczone do pracy ciągłej w serwerach, każdy o pojemności co najmniej 240GB oraz MTBF co najmniej 2mln godzin. Dwa dyski twarde przeznaczone do pracy ciągłej w serwerach, każdy o pojemności co najmniej 1TB i 64MB pamięci Cache.
Obudowa	Obudowa Tower. Minimum cztery wewnętrzne zatoki 3,5" umożliwiające beznarzędziowy montaż dysków twardych.

	Jeden zasilacz o mocy co najmniej 350W
Porty	Na przednim panelu: 2 x USB, na tylnym panelu: 1 x RS-232, 2 x USB 3.0, 1 x VGA, 2x RJ45. Wewnątrz serwera co najmniej jedno złącze USB 3.0 Typ A.
Certyfikaty	Certyfikat PN-EN ISO 9001:2001(ISO 9001:2001) na procesy projektowania, produkcję, sprzedaż i serwis, PN-EN ISO14001:2005 (ISO 14001:2005) oraz PN-ISO/IEC 27001:2007 lub nowsze Deklaracja producenta o zgodności z dyrektywami LVD 2006/95/WE oraz Dyrektywy EMC 2004/108/WE. Deklaracja producenta sprzętu o zgodności oferowanego serwera z wymaganiami normy Energy Star 2.0. Wymagane potwierdzenie obecności oferowanego modelu na stronie internetowej Energy Star przez dostarczenie wydruku ze strony http://www.eu-energystar.org z kategorii Enterprise server.
Wsparcie techniczne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego.

4.) Serwer –Serwer plików - 3szt

Parametr	**Opis**
Informacje podstawowe Typ obudowy	Tower
Pojemność zainstalowanej pamięci	min.1024 MB
Ilość zainstalowanych dysków	min 1 szt. 1TB przeznaczony do pracy ciągłej
Maksymalna ilość dysków	min 2 szt.
Poziomy RAID	0 , 1, JBOD
Karta sieciowa	2 x 10/100/1000 Mbit/s
Ilość wolnych kieszeni 3,5 (wewnętrznych)	min 2 szt.
Ilość wolnych kieszeni 2,5 (wewnętrznych)	min 2 szt.
Ilość półek na dyski Hot Swap	min 2 szt.
Interfejsy	min 3 x USB 3.0, 2 x RJ-45, 1x Kensington Lock konektor
Ilość zasilaczy	min 1szt
Moc zasilacza	max66 Wat
Obsługiwane protokoły i standardy	CIFS/SMB, AFP 3.3, NFS, FTP/FTPS, SFTP, TFTP, http, HTTPS, Telnet, iSCSI, SSH, SNMP, SMTP, SMSC, TCP/IP, DHCP Client, DHCP Server, UPnP, Bonjour, DNS, LDAP
zarządzanie	Web File Management
Informacje – pozostałe	Wake-On-LAN , S.M.A.R.T.

Obsługiwane systemy operacyjne	Windows 7, Linux, Mac OS X, UNIX, Windows Server, Windows 8, Windows 10
Wymiary	max 103 mm x169 mm x 226 mm
Masa netto max	1,28 kg

5.) Router -8 szt

Porty:	min 4 x LAN100/1000Mb/s , 1x WAN 100/1000Mb/s 1x USB 3.0 1x USB 2.0
Przycisk:	WPS/RESET, Wyłącznik, wyłącznik sieci WiFI
Antena:	Antena: możliwość podłączenia 3 dwupasmowych anten zewnętrznych
Wymiary:	max222 x 87 x 169mm
Częstotliwość pracy:	min 2,4GHz oraz 5GHz
Standardy bezprzewodowe:	IEEE 802.11ac/n/a 5GHz, IEEE 802.11b/g/n 2,4GHz
Czułość odbiornika 5GHz	11a 6Mb/s-96dBm, 11a 54Mb/s: -79dBm, 11ac HT20: -71dBm, 11ac HT40:
Czułość odbiornika 2,4 GHz	11g 54M: -77dBm 11n HT20: -74dBm 11n HT40: -72dBm
EIRP CE:	<20dBm(2,4GHz)<23dBm(5GHz)
Funkcje transmisji bezprzewodowej	WDS bridge, WMM, Statystyki transmisji bezprzewodowej
Bezpieczeństwo transmisji bezprzewodowej:	min WEP 64/128 bit, WPA /WPA2, szyfrowanie WPA-PSK/WPA2-PSK
Funkcja	Quality of Service WMM, Kontrola przepustowości
Sieć WAN Dynamiczne IP/Statyczne IP/PPPoE/	
PPTP(Dual Access)/L2TP(Dual Access)/BigPond	
Zarządzanie:	Kontrola dostępu, Zarządzanie lokalne, Zarządzanie zdalne
DHCP:	Serwer, Klient, Lista klientów DHCP, Rezerwacja adresów
Przekierowanie portów:	Serwery wirtualne, Port Triggering, DMZ, UPnP
Kontrola dostępu :	Kontrola rodzicielska, lokalna kontrola dostępu do panelu zarządzania, lista hostów, harmonogram dostępu, zarządzanie regułami
Zabezpieczenia zapory sieciowej:	Ochrona przed atakami DoS, zapora sieciowa SPI, filtrowanie domen, adresów IP i MAC, wiązanie adresów IP i MAC
Protokoły:	IPv4 oraz IPv6
Udostępnianie urządzeń USB	Serwer Samba(udostępnianie dysków)/Serwer FTP/Serwer multimediów/Serwer druku
Funkcja Guest Network Jedna sieć dla gości w paśmie 2,4GHz	
Jedna sieć dla gości w paśmie 5GHz	
Wymagania systemowe	Microsoft Windows 98SE, NT, 2000, XP, Vista™ lub Windows 7, Windows 8, MAC OS, NetWare, UNIX lub Linux
Zestaw powinien zawierać	min 3 anteny, Instrukcja szybkiej instalacji, Płyta CD, Zasilacz 12V

6.) Monitor interaktywny- 5 szt

Przekątna	65"
Rozdzielczość	1920x1080
Jasność (cd/m2)	Min. 350
Kontrast	Min. 3000:1

Technologia dotyku		Podczerwień
Pkt dotyku		Min. 4
Szyba		Min. 4 mm
Wejścia video:		
	HDMI	Min. 2
	VGA	Min. 1
	DVI-D	Min. 1
	DP	Min. 1
Wyjścia Video		
	DP	Min. 1
	VGA	Min. 1
Wejścia Audio		
	3,5mm jack	Min. 1
	Audio Lewy / Prawy	RCA
Wyjścia audio		
	Audio Lewy / Prawy	RCA
	na zewnętrzne głośniki	Min. 1
Komunikacja		
	RS232	Min. 1
	RJ45	Min. 1
	USB	Min. 1
	Slot OPS	Min. 1
Głośniki		2 x min. 10W
Zużycie prądu		Maks. 230W
Deklarowana przez producenta żywotność panelu		Min. 50 000 h
Oprogramowanie wybrane minimalne wymagania		
	interaktywne narzędzia:	Rysowanie funkcji matematycznych
		Ekierka, Cyrkiel, Kątomierz, Linijka
		Kurtyna, Reflektor
		Zegar, Minutnik
		Nagrywanie ekranu
	tworzenie interaktywnych ćwiczeń z możliwością weryfikacji poprawności ich wykonania	Dopasowywanie obrazków
		Kolejność obrazów
		Kolejność słów
		Kolejność zdań
		Kategoryzacja obrazków
		Kategoryzacja tekstu
		Rozdzielanie zdań
		Sylaby
		Matematyczne ćwiczenia, t.j. Kółko I krzyżyk, memory, działania, tabliczka (mnożenie, dzielenie, dodawanie, odejmowanie)
		Test jednokrotnego wyboru
	biblioteka zasobów	audio, video, flash, obrazy

	tryby pracy	jeden użytkownik, dwóch, trzech, czterech użytkowników (indywidualne paski narzędziowe oraz podział na strefy)
		tryb prezentacji
		tryb wieloekranowy
	dostęp do bazy Otwartych Zasobów Edukacyjnych	tak

7.) Laptop- 83 szt

Parametr	Opis
Ekran	TFT 15.6" LED HD o rozdzielczości 1366x768, z powłoką matową, nie dopuszcza się matryc typu "glare".
Wydajność/ Procesor	Procesor dwurdzeniowy uzyskujący wynik co najmniej 3830 punktów w teście Passmark - CPU Mark według wyników procesorów publikowanych na stronie http://www.cpubenchmark.net/cpu_list.php (na dzień nie wcześniejszy niż 01.10.2016). W ofercie wymagane podanie producenta i modelu procesora. 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. - Klapa serwisowa umożliwiająca bezpośredni dostęp do dysków HDD, SSD oraz pamięci ram, bez konieczności odkręcania całej dolnej pokrywy notebooka
Pamięć RAM	6GB (1x 4 GB DDR4 RAM + 1x 2 GB DDR4 RAM)
Dysk twardy	1x 500 GB SATA, prędkość obrotowa 5400 obr./min. (możliwość montażu dodatkowego dysku SSD na złączu M2)
	Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.: - systemu operacyjnego - oprogramowania biurowego - oprogramowania antywirusowego Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.
Karta graficzna	Zintegrowana ze wspraciem dla OpenGL 4.4, OpenCL 2.0, Microsoft DirectX 12. Powinna osiągać w teście wydajności: PassMarkPerformanceTest wynik min. 820 punktów w G3D Rating (wynik dostępny: http://www.videocardbenchmark.net/gpu_list.php) (na dzień nie wcześniejszy niż 01.10.2016)
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 Ethernet RJ 45 (WOL) - WLAN 802.11 ac wraz z Bluetooth 4.2 COMBO
Porty/złącza (wbudowane)	1 x Złącze RJ-45 (podłączenie sieci lokalnej) 1 x Czytnik Kart pamięci SD™ 2 x USB 3.0 (1 port z możliwością ładowania przy wyłączonym notebooku) 1 x USB 2.0 1 x USB 3.1 Type-C port 1 x VGA (D-Sub), 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
Kamera	Wbudowana, o parametrach: - HD 1280 x 720 rozdzielczość - 720p HD audio/video nagrywanie - High Dynamic Range Imaging (HDR)

Napęd optyczny (wbudowany)	8x DVD +/- RW Super Multi Dual Layer wewnętrzny (z oprogramowaniem do nagrywania płyt DVD oraz odtwarzania płyt DVD Video).
Bateria	Litowo-jonowa 4 komorowa 41 Wh 2800 mAh – czas pracy min. 8h według karty katalogowej producenta.
Zasilacz	Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 65W.
Waga i wymiary	- Waga max do 2250 g z baterią i napędem optycznym, - Wymiary 382 (szerokość) x 260 (głębokość) x 24/31 (wysokość) mm
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 w miejscu instalacji sprzetu. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. b) Gwarancja na baterię min. 12 miesięcy. c) Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie producenta sprzętu (lub jego przedstawiciela w Polsce) potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta. d) Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera. e) Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001 – należy dołączyć dokument potwierdzający, że serwis urządzeń będzie realizowany zgodnie z tą normą. f) 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 desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Interfejs graficzny użytkownika pozwalający na obsługę: a. Klasyczną przy pomocy klawiatury i myszy, b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim, 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe, 4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje, 5. Wbudowany system pomocy w języku polskim; 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.

	8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne, 10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 15. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 16. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 17. 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, 18. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 19. Obsługa standardu NFC (near field communication), 20. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 21. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 22. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 23. Mechanizmy uwierzytelniania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), 24. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 25. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji, 26. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od

	wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku 27. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym, 28. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 29. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 30. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 31. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, 32. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, 33. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
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, Windows 8 oraz Windows 7 (załączyć wydruk ze strony Microsoft WHCL). - Oferowany model notebooka musi być zgodny z normą Energy Star 5.0 (załączyć wydruk ze strony Energy Star). - 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 – 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 mputera. C) Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego: zgłoszenie awarii sprzętu, zgłoszenie zapytania technicznego. D) 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.
Oprogramowanie biurowe	Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 13. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej, 14. Wymagania odnośnie interfejsu użytkownika: a. Pełna polska wersja językowa interfejsu użytkownika.

	b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 15. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: 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. 16. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji. 17. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy). 18. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim. 19. Pakiet zintegrowanych aplikacji biurowych musi zawierać: 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. 20. Edytor tekstów musi umożliwiać: a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. b. Wstawianie oraz formatowanie tabel. c. Wstawianie oraz formatowanie obiektów graficznych. d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. f. Automatyczne tworzenie spisów treści. g. Formatowanie nagłówków i stopek stron. h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.

	i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. j. Określenie układu strony (pionowa/pozioma). k. Wydruk dokumentów. l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem. p. 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. 21. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice) e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych g. Wyszukiwanie i zamianę danych h. Wykonywanie analiz danych przy użyciu formatowania warunkowego i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności

	k. Formatowanie czasu, daty i wartości finansowych z polskim formatem l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. m. 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. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 22. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. 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. 23. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a. Tworzenie i edycję drukowanych materiałów informacyjnych b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów. c. Edycję poszczególnych stron materiałów. d. Podział treści na kolumny. e. Umieszczanie elementów graficznych. f. Wykorzystanie mechanizmu korespondencji seryjnej. g. Płynne przesuwanie elementów po całej stronie publikacji. h. Eksport publikacji do formatu PDF oraz TIFF. i. Wydruk publikacji.

	j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 24. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, c. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, d. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, e. Automatyczne grupowanie poczty o tym samym tytule, f. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów, h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie, i. Zarządzanie kalendarzem, j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, k. Przeglądanie kalendarza innych użytkowników, l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, m. Zarządzanie listą zadań, n. Zlecanie zadań innym użytkownikom, o. Zarządzanie listą kontaktów, p. Udostępnianie listy kontaktów innym użytkownikom, q. Przeglądanie listy kontaktów innych użytkowników, r. Możliwość przesyłania kontaktów innym użytkowników, s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
Oprogramowanie Antywirusowe	88. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 89. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 90. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. 91. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.

	92. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives **Ochrona antywirusowa i antyspyware** 93. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 94. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 95. Wbudowana technologia do ochrony przed rootkitami. 96. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 97. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 98. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 99. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. 100. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 101. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 102. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. 103. Możliwość skanowania dysków sieciowych i dysków przenośnych. 104. Skanowanie plików spakowanych i skompresowanych. 105. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 106. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 107. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 108. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 109. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 110. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 111. 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.

	112. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). 113. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 114. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 115. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 116. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 117. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 118. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. 119. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. 120. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 121. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 122. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 123. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 124. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 125. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 126. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 127. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 128. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. 129. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi

	wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 130. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 131. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 132. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 133. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 134. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 135. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 136. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 137. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 138. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. 139. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 140. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 141. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 142. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 143. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej:

	Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu. 144. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 145. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. 146. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 147. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 148. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 149. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 150. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 151. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach. • Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 152. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

	153. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 154. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 155. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 156. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 157. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 158. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 159. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 160. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 161. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 162. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 163. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 164. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 165. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 166. Program ma być w pełni zgodny z technologią CISCO Network Access Control. 167. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. 168. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 169. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. 170. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron

	Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 171. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 172. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. 173. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 174. Możliwość podejrzenia licencji za pomocą, której program został aktywowany. Ochrona serwera plików Windows 68. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016 SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. 69. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 70. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 71. Wbudowana technologia do ochrony przed rootkitami i exploitami. 72. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 73. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 74. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 75. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 76. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. 77. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 78. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 79. Możliwość skanowania dysków sieciowych i dysków przenośnych. 80. Skanowanie plików spakowanych i skompresowanych. 81. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 82. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku

	wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 83. Aplikacja powinna wspierać mechanizm klastrowania. 84. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 85. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 86. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 87. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire. 88. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 89. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika. 90. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. 91. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 92. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 93. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 94. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 95. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 96. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 97. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 98. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 99. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 100. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 101. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

	102. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 103. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. 104. Aktualizacje modułów analizy heurystycznej. 105. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 106. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 107. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych. 108. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 109. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 110. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 111. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 112. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. 113. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 114. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. 115. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. 116. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim

	priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu. 117. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 118. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 119. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 120. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB. 121. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 122. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 123. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 124. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 125. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 126. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 127. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 128. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu. 129. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 130. Aplikacja musi wspierać skanowanie magazynu Hyper-V 131. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 132. Praca programu musi być niezauważalna dla użytkownika.

	133. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania. 134. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna** 90. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. 91. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 92. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 93. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. 94. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 95. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 96. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. 97. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 98. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 99. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. 100. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 101. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 102. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 103. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. 104. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 105. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 106. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym. 107. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 108. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz

	sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. 109. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. 110. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 111. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 112. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. 113. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. 114. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 115. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 116. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. 117. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej 118. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 119. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 120. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. 121. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny. 122. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 123. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. 124. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

	125. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 126. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. 127. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 128. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej 129. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 130. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. 131. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 132. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 133. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 134. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. 135. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 136. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. 137. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup. 138. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 139. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 140. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji. 141. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium

	producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 142. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. 143. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 144. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 145. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. 146. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. 147. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 148. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. 149. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. 150. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. 151. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 152. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 153. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora. 154. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta 155. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów. 156. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.

	157. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 158. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp. 159. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kołumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania. 160. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów. 161. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. 162. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 163. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 164. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. 165. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. 166. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 167. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 168. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. 169. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. 170. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 171. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 172. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 173. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.

	174. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 175. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 176. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. 177. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. 178. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 179. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).

8.) Projektor multimedialny + ekran – 50 szt.

Parametr	**Opis**
Technologia	LCD
Jasność	minimum 2700 ANSI lumenów w trybie pełnej jasności
Kontrast	minimum 2000
Rozdzielczość rzeczywista	minimum 1024x768, format matrycy 4
Wbudowany obiektyw ZOOM	
Współczynnik odległości do szerokości obrazu	o minimalnym zakresie 1,5 – 1,8
Wielkość obrazu	minimalnym zakresie 30 – 300 cali
Odległość od ekranu	minimalnym zakresie 0,9 – 10,9 m
Zakres elektronicznej korekcji efektu trapezowego	w pionie +/- 30 stopni
Żywotność lampy	min 5000 godzin w trybie pełnej jasności / 10000 w trybie ECO2
Porty wejścia minimum.	1 x HDMI, 2 x VGA (DB-15), 1 x composite video (RCA Chinch),2 x audio stereo mini Jack 1 x audio stereo 2RCA 1 x RS232 1 x RJ45 1 x USB typ B
Porty wyjścia min	1 x VGA (DB-15), 1 x audio stereo mini Jack
Waga	max 3,1 kg
Głośność pracy	(max) 37dB w trybie pełnej jasności
Moc wbudowanych głośników	min 16W
Zabezpieczenia antykradzieżowe kodem PIN	
Filtr powietrza, który użytkownik sam może wymienić i wyczyścić bez konieczności demontażu projektora i użycia narzędzi	
Wymiana lampy bez konieczności demontażu projektora	
Co najmniej 2 uchwyty do montażu mechanicznych zabezpieczeń przeciw kradzieżowych – przygotowane przez producenta projektora	
Ekranu	Rozwijany ręcznie
Wymiary ekranu	min 200 x 200 cm
Format	4:3
Przekątna obrazu:	min 96 [cale]

Czarne ramki boczne	Max 2.6 cm
Wymiary obrazu	Min 194 x 146 cm
Czarny TOP	max 49.5 cm
Czarny dół	max 4 cm
Przekrój kasety:	max 7.2 x 7.2 cm
Materiał obudowy	Stal
Rodzaj powierzchni	Matt White
Waga netto:	max 6.6 kg

9.) Kamera – 1szt

Parametr	**Opis**
format nośnika:	min SDXC SDHC SD
złącza:	wyjście AV miniUSB , HDMI (mini) wyjście słuchawkowe
jakość nagrywania filmów:	min Full HD
format nagrywania:	min AVCHD|MP4
rozdzielczość wideo	min. 1920 x 1080|1440 x 1080|1280 x 720
ogniskowa obiektywu	2,8 - 89,6 mm
ogniskowa obiektywu wg filmu 35mm	32,5 - 1853 mm
zoom cyfrowy:	1140 x
zoom optyczny:	32 x
przysłona min 1.8 max 4.5	
szybkość migawki (min)	1/2 s
szybkość migawki (max)	1/2000 s
wyświetlacz LCD	3 cali
zastosowany akumulator	litowo-jonowy
Wymiary:	max 54 mm x 59 mm x117 mm
Waga:	max 241 g

10.) Aparat Fotograficzny – 1szt

Parametr	**Opis**
Rozdzielczość	Min 20 Mpix
Zbliżenie optyczne	50 x Zbliżenie cyfrowe 200 x
Ogniskowa (dla 35 mm)	min 24 - 1200 mm
Jasność	f/2.8-6.3
Ustawianie ostrości	od min 1 cm
Optyczna stabilizacja obrazu	
Obsługa w języku polskim	
Ręczne i automatyczne ustawianie ostrości	
Funkcje dodatkowe	automatyczny wybór programu tematycznego, technologia rozpoznawania twarzy, technologia wykrywania uśmiechu, dźwięk stereo, funkcja panoramy, tryby kreatywne i efekty artystyczne, funkcje poprawy jakości i edycji zdjęć, funkcja Skin Soften, automatyczna regulacja jasności wyświetlacza LCD,
Wielkość ekranu LCD	min 3 " ruchomy ekran
Wizjer elektroniczny	
Wbudowana lampa błyskowa	

Tryby pracy lampy błyskowej	
Zapis	SD, SDHC, SDXC, microSD, Memory Stick Duo, Memory Stick Pro Duo, Memory Stick PRO Duo High Speed, Memory Stick PRO-HG Duo, microSDHC wbudowana pamięć min 48MB zapis zdjęć w formacie
Rodzaj przetwornika	CMOS Exmor R 1/2,3"
Nagrywanie filmów z dźwiękiem w jakości min Full HD (1920 x 1080)	
Czas otwarcia migawki	Min. 30 - 1/4000 s
Ustawienia	automatyczny, duża czułość, gładka skóra, krajobraz, miękkie zdjęcie, plaża, portret nocą, sceneria nocna, sport, sztuczne ognie, śnieg, zwierzęta, Zdjęcia seryjne, możliwość ręcznej i automatycznej ustawienie czułości
Zakres czułości ISO	min80 – 12800
Balans bieli	automatyczny, ręczny
Korekcja ekspozycji	
Wyjścia	micro HDMI (typ D), usb 2.0 AV
Wymiary	max 131 x 94 x 103 mm
Waga (bez baterii)	max 628 g
Zasilanie	akumulatorem litowym
Wyposażenie	oprogramowanie, pasek, pokrywa na obiektyw, kabel USB, zasilacz sieciowy, instrukcja obsługi w języku polskim,

11.) Modernizacja i rozbudowa sieci komputerowej w Szkole Podstawowej nr 2 im. Ks. Jana Twardowskiego – 1szt

Podstawowe założenia:

a) Wszystkie prace należy wykonać w oparciu o obowiązujące przepisy i zasady określone w PN-EN 50173-1.
b) Zamawiający zaleca przeprowadzenie wizji technicznej przed złożeniem oferty celem dokładnego oszacowania ilości materiałów niezbędnych do wykonania zadania oraz dokonania niezbędnych uzgodnień.
c) Wszelkie usterki wynikłe podczas prowadzenia prac przy modernizacji i rozbudowie Wykonawca przywróci do stanu pierwotnego na własny koszt.

Serwer:

a) w ramach modernizacji i rozbudowy sieci komputerowej Wykonawca dostarczy jeden serwer, zainstaluje i skonfiguruje go do prawidłowego działania w tym zapewni mechanizm tworzenia kopii zapasowych ważnych danych.
b) oprogramowanie serwera ma posiadać możliwość pracy jako kontroler domeny. Zarządzanie użytkownikami domeny, tworzenie kopii zapasowych ich plików.
c) modyfikacja praw dostępu do danych i aplikacji dostępnych dla użytkowników ma się odbywać centralnie na serwerze.
d) użytkownicy logujący się do serwera mają możliwość umieszczania własnych danych na dyskach sieciowych przypisanych do ich konta, oraz na ogólnodostępnym dysku sieciowym.
e) Serwer ma posiadać funkcję udostępniania drukarki w sieci lokalnej.

Sieć logiczna:

a) trasy prowadzenia okablowania poziomego jak i pionowego należy skoordynować z istniejącymi instalacjami w budynku m.in. instalacją elektryczną, instalacją centralnego ogrzewania, wody, gazu, itp.

b) prace należy prowadzić w czasie niekolidującym z przeprowadzaniem zajęć lekcyjnych
c) na terenie szkoły Wykonawca wybuduje dwa punkty dystrybucyjne PD1, PD2 wyposażone odpowiednio w:
   - szafę wiszącą 12U z półką i przeszklonymi drzwiami
   - patch panel 2x 24porty
   - przełącznik sieciowy 2x 24porty
   - router WiFi
   - listwę zasilającą zamontowaną na szynach szafy rack
   - półkę
   - organizator kabli rack 1U
d) do przynajmniej jednego punktu dystrybucyjnego należy doprowadzić przyłącz z istniejącego łącza internetowego zlokalizowanego na terenie szkoły
e) PD1 należy połączyć z PD2 zachowując standardy budowy sieci logicznej według Polskie Normy PN-EN 50173-1
f) w ramach przedmiotowego zamówienia Wykonawca zmodernizuje i rozbuduje istniejącą infrastrukturę sieci logicznej na terenie obiektu Klienta:
   - wymiana, montaż do 24 gniazd abonenckich dwóch pracowniach komputerowych
   - wymiana, dobudowa okablowania do 24 gniazd abonenckich w pracowniach komputerowych
   - doprowadzenie po jednej korespondencji logicznej zakończonej gniazdem abonenckim do 18 sal lekcyjnych na terenie Szkoły (po za pracowniami komputerowymi) zachowując standardy budowy sieci logicznej według normy PN-EN 50173-1. Okablowanie należy układać w korytach PCV. Wszelakie przejścia przez ściany należy doprowadzić do stanu pierwotnego.
   - okablowanie od gniazd abonenckich należy doprowadzić do wyposażonych szaf dystrybucyjnych PD1, PD2 zgodnie z powyższym opisem.
   - konfiguracja sieci LAN
g) minimalne wymagania gniazd abonenckich:
   - standard 45x45
   - gniazdka dwumodułowe z mocowaniami typu keystone z przesłonkami
   - pole opisowe
   - montaż na wcisk

Sieć WiFi:

a) w ramach modernizacji i rozbudowy sieci Zamawiający wymaga zainstalowania na terenie swojego obiektu 6 punktów dostępowych schodzących się w punkcie dystrybucyjnym PDW1
b) Wykonawca przedstawi Zamawiającemu planowanie radiowe zasięgu sieci WiFi z graficznym pokryciem obszaru zaprojektowanych urządzeń na podkładzie (rzucie) który pozyska od Zamawiającego.
c) punkty dostępowe zasilane w technologii PoE
d) standard sieci 802.11 b/g/n
e) częstotliwość WiFi 2.4GHz
f) szyfrowanie: WPA2, WPA, 64/128 bit WEP
g) dostęp do sieci wymaga autoryzacji
h) poprzez utworzenie segmentów VLAN należy wydzielić odrębne sieci w uzgodnieniu z Zamawiającym.
i) możliwość konfiguracji kilku sieci WIFI, w tym sieci dla gości, logowanie gościa za pomocą jednorazowego hasła z ustawionym czasem dostępu do sieci,
j) automatyczne przełączanie pomiędzy punktami dostępu,
k) zarządzanie wszystkimi punktami dostępowymi za pomocą jednego centralnego kontrolera zabezpieczonego hasłem i dostępnego przez przeglądarkę internetową,

l) na terenie szkoły Wykonawca wybuduje odrębny punkt dystrybucyjny PDW1 dla sieci WiFi wyposażony odpowiednio w:

- szafę rack wiszącą, z przeszklonymi drzwiami co najmniej 6U z półką
- patch panel 8 portowy
- listwę zasilającą zamontowaną na szynach szafy rack

m) do punktu dystrybucyjnego należy doprowadzić Internet od najbliższego dostępnego urządzenia aktywnego.

n) w punkcie dystrybucyjnym ma być zamontowany zarządzany przełącznik sieciowy do którego zostaną wpięte punkty dostępowe, kontroler sieci WiFi i sieć Internet, przełącznik ma posiadać funkcję zasilania urządzeń w technologii POE oraz tworzenia VLAN

Charakterystyka urządzeń:

SERWER	
Parametr	**Charakterystyka**
Płyta główna	Serwerowa, jednoprocesorowa z możliwością instalacji modułu TPM
Procesor	Jeden procesor przynajmniej 4-rdzeniowy taktowany zegarem minimum 2,26 GHz posiadający pamięć podręczną cache o wielkości przynajmniej 8MB.
Zarządzanie	Zintegrowany moduł zarządzający z dedykowanym portem RJ45 i pełnym przekierowaniem konsoli KVM
Złącza kart rozszerzeń	Minimum 1x PCI-E 3.0 x8 (x16 slot), 1x PCI-E 3.0 x8 oraz 1x PCI-E 3.0 x4 (x8 slot)
Pamięć	Co najmniej 8GB RAM, możliwość rozbudowy do 64GB,
Karta sieciowa	Dwa porty 1Gb Ethernet (niezależne od karty zarządzającej), obsługa startu z iSCSI oraz PXE
Karta graficzna	Zintegrowana z płytą główną
Kontroler RAID	Zintegrowany z płytą główną kontroler SATA RAID 0,1,10, posiadający co najmniej sześć złącz SATA 6Gbps
Dysk twardy	Dwa dyski SSD przeznaczone do pracy ciągłej w serwerach, każdy o pojemności co najmniej 240GB oraz MTBF co najmniej 2mln godzin. Dwa dyski twarde przeznaczone do pracy ciągłej w serwerach, każdy o pojemności co najmniej 1TB i 64MB pamięci Cache.
Obudowa	Obudowa Tower. Minimum cztery wewnętrzne zatoki 3,5" umożliwiające beznarzędziowy montaż dysków twardych. Jeden zasilacz o mocy co najmniej 350W
Porty	Na przednim panelu: 2 x USB, na tylnym panelu: 1 x RS-232, 2 x USB 3.0, 1 x VGA, 2x RJ45. Wewnątrz serwera co najmniej jedno złącze USB 3.0 Typ A.
Certyfikaty	Certyfikat PN-EN ISO 9001:2001(ISO 9001:2001) na procesy projektowania, produkcję, sprzedaż i serwis, PN-EN ISO14001:2005 (ISO 14001:2005) oraz PN-ISO/IEC 27001:2007 lub nowsze Deklaracja producenta o zgodności z dyrektywami LVD 2006/95/WE oraz Dyrektywy EMC 2004/108/WE. Deklaracja producenta sprzętu o zgodności oferowanego serwera z wymaganiami normy Energy Star 2.0. Wymagane potwierdzenie obecności oferowanego modelu na stronie internetowej Energy Star przez dostarczenie wydruku ze strony http://www.eu-energystar.org z kategorii Enterprise server.
Wsparcie techniczne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej

	producenta numeru seryjnego.
Oprogramowanie	Oprogramowanie serwera ma posiadać możliwość pracy jako kontroler domeny. Zarządzanie użytkownikami domeny, tworzenie kopii zapasowych ich plików, modyfikacja praw dostępu do danych i aplikacji dostępnych dla użytkowników ma się odbywać centralnie na serwerze. Użytkownicy logujący się do serwera mają możliwość umieszczania własnych danych na dyskach sieciowych przypisanych do ich konta, oraz na ogólnodostępnym dysku sieciowym. Serwer ma posiadać funkcję udostępniania drukarki w sieci lokalnej.

MONITOR DO SERWERA	
Parametr	**Charakterystyka**
Przekątna ekranu	Min 21,5 cali
Zalecana rozdzielczość obraz	Min 1920 x 1080 pikseli
Czas reakcji matrycy	Min 5 ms
Jasność	Min 200 cd/m2
Kąt widzenia poziomy	Min 90 stopni
Kąt widzenia pionowy	Min 65 stopni
Pobór mocy (praca/spoczynek)	Min 19/0,5 Wat
Montaż na ścianie (VESA)	Min 100 x 100 mm

SZAFA RACK	
Parametr	**Charakterystyka**
Kolor	RAL9004 Czarny
Masa netto:	max 21. kg
Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją	
przepusty kablowe	min. jeden w suficie, drugi w podłodze
Wymiary:	450 mm x 600 mm x 638 mm
Wysokość wewnętrzna:	12U

PRZEŁĄCZNIK SIECIOWY	
Parametr	**Charakterystyka**
liczba portów 1000 Mbit	Min 24 szt.
typ	zarządzalny
przeznaczenie	do szaf RACK 19"
obsługiwane protokoły	IEEE 802.3u, IEEE 802.3i, IEEE 802.3ab, IEEE 802.3, IEEE 802.1Q, IEEE 802.1p
rozmiar tablicy adresów MAC	Min 8000
algorytm przełączania	store-and-forward
prędkość magistrali wew.	Min 48 Gb/s
obsługa VLANów	
Wymiary	Max 294 mmx 45mm x 180 mm

ROUTER WiFi	
Parametr	**Charakterystyka**
Porty:	min 4 x LAN100/1000Mb/s , 1x WAN 100/1000Mb/s 1x USB 3.0 1x USB 2.0

Przycisk:	WPS/RESET, Wyłącznik, wyłącznik sieci WiFI
Antena:	Antena: możliwość podłączenia 3 dwupasmowych anten zewnętrznych
Wymiary:	max222 x 87 x 169mm
Częstotliwość pracy:	min 2,4GHz oraz 5GHz
Standardy bezprzewodowe:	IEEE 802.11ac/n/a 5GHz, IEEE 802.11b/g/n 2,4GHz
Czułość odbiornika 5GHz	11a 6Mb/s-96dBm, 11a 54Mb/s: -79dBm, 11ac HT20: -71dBm, 11ac HT40:
Czułość odbiornika 2,4 GHz	11g 54M: -77dBm 11n HT20: -74dBm 11n HT40: -72dBm
EIRP CE:	<20dBm(2,4GHz)<23dBm(5GHz)
Funkcje transmisji bezprzewodowej	WDS bridge, WMM, Statystyki transmisji bezprzewodowej
Bezpieczeństwo transmisji bezprzewodowej:	min WEP 64/128 bit, WPA /WPA2, szyfrowanie WPA-PSK/WPA2-PSK
Funkcja	Quality of Service WMM, Kontroła przepustowości
Sieć WAN Dynamiczne IP/Statyczne IP/PPPoE/	
PPTP(Dual Access)/L2TP(Dual Access)/BigPond	
Zarządzanie:	Kontrola dostępu, Zarządzanie lokalne, Zarządzanie zdalne
DHCP:	Serwer, Klient, Lista klientów DHCP, Rezerwacja adresów
Przekierowanie portów:	Serwery wirtualne, Port Triggering, DMZ, UPnP
Kontrola dostępu :	Kontrola rodzicielska, lokalna kontrola dostępu do panelu zarządzania, lista hostów, harmonogram dostępu, zarządzanie regułami
Zabezpieczenia zapory sieciowej:	Ochrona przed atakami DoS, zapora sieciowa SPI, filtrowanie domen, adresów IP i MAC, wiązanie adresów IP i MAC
Protokoły:	IPv4 oraz IPv6
Udostępnianie urządzeń USB	Serwer Samba(udostępnianie dysków)/Serwer FTP/Serwer multimediów/Serwer druku
Funkcja Guest Network Jedna sieć dla gości w paśmie 2,4GHz	
Jedna sieć dla gości w paśmie 5GHz	
Wymagania systemowe	Microsoft Windows 98SE, NT, 2000, XP, Vista™ lub Windows 7, Windows 8, MAC OS, NetWare, UNIX lub Linux
Zestaw powinien zawierać	min 3 anteny, Instrukcja szybkiej instalacji, Płyta CD, Zasilacz 12V

PRZEŁĄCZNIK SIECIOWY PoE	
Parametr	**Charakterystyka**
Porty	9 portów 10/100Mb/s (8 x PoE + 1 x UPLINK)
Zasilanie PoE	IEEE 802.3af (porty 1÷8), 48VDC / max 15,4W na każdy port
Protokoły, Standardy	IEEE802.3, 802.3u, 802.3x CSMA/CD, TCP/IP
Przepustowość	Min 1,6Gbps
Optyczna sygnalizacja pracy	Zasilanie switch'a; Link/Act; PoE Status
Zasilanie	90 ÷ 264VAC 50÷60Hz / 2,5A 230VAC zasilacz typu desktop PSD 480250 48VDC / 2,5A/120W max.
Wymiary	Max 191 x 29 x 116 [mm]

ACCESS POINT	
Parametr	**Charakterystyka**
Częstotliwość	2,4 GHz
Praca w standardzie	802.11 b/g/n
Zasilanie	PoE
wymiary	max: 201x201x37mm
Montaż	Ściana, sufit
Porty	min 1x Ethernet 10/100
Bezpieczeństwo	WEP,WPA-PSK,WPA-TKIP,WPA2-AES
Wskaźnik zasilania	LED
Antena	2x2MIMO
Zużycie mocy	Max 4.1 W
Konfiguracja	Przeglądarka WWW, dedykowany kontroler

KONTROLER	
Parametr	**Charakterystyka**
Pojemność dysku wewnętrznego	Min 0.1 TB
Łączność	LAN (10,100,1000 Mbit/s), USB
Napięcie wyjściowe adaptera AC	Min 5 V
Wymiary	Max 21,8x44x122
Waga	112g
Zasilacz dołączony do zestawu	

12.) Urządzenie wielofunkcyjne – 1 szt.

Parametr	**Charakterystyka**
Obsługiwany typ nośnika	min. etykiety, koperty, papier zwykły
Technologia druku	Laserowa
Obsługiwany format nośnika	min. B6, B5, A6, A5, A4
Podajnik papieru	min. 150 arkuszy
Odbiornik papieru	min 100 arkuszy
Minimalna rozdzielczość druku	600 x 600 dpi
Minimalna rozdzielczość skanowania	1200x 1200 dpi
Szybkość druku w czerni	min. 22 str/min
Funkcja faksu	TAK
Szybkość skanowania	max. 3 sek.
Zainstalowana pamięć	min. 256 MB
Prędkość procesora	min. 600 MHz
Podajnik dokumentów ADF	TAK
Interfejsy	min RJ

13.) Projektor - 15szt

Parametr	Opis
Technologia	LCD

Jasność	minimum 2700 ANSI lumenów w trybie pełnej jasności
Kontrast	minimum 2000
Rozdzielczość rzeczywista	minimum 1024x768, format matrycy 4
Wbudowany obiektyw ZOOM	
Współczynnik odległości do szerokości obrazu	o minimalnym zakresie 1,5 – 1,8
Wielkość obrazu	minimalnym zakresie 30 – 300 cali
Odległość od ekranu	minimalnym zakresie 0,9 – 10,9 m
Zakres elektronicznej korekcji efektu trapezowego	w pionie +/- 30 stopni
Żywotność lampy	min 5000 godzin w trybie pełnej jasności / 10000 w trybie ECO2
Porty wejścia minimum.	1 x HDMI, 2 x VGA (DB-15), 1 x composite video (RCA Chinch),2 x audio stereo mini Jack 1 x audio stereo 2RCA 1 x RS232 1 x RJ45 1 x USB typ B
Porty wyjścia min	1 x VGA (DB-15), 1 x audio stereo mini Jack
Waga	max 3,1 kg
Głośność pracy	(max) 37dB w trybie pełnej jasności
Moc wbudowanych głośników	min 16W
Zabezpieczenia antykradzieżowe kodem PIN	
Filtr powietrza, który użytkownik sam może wymienić i wyczyścić bez konieczności demontażu projektora i użycia narzędzi	
Wymiana lampy bez konieczności demontażu projektora	
Co najmniej 2 uchwyty do montażu mechanicznych zabezpieczeń przeciw kradzieżowych – przygotowane przez producenta projektora	

14.) Ekran – 15szt

Parametr	Opis
Typ ekranu	Na trójnogu
Wymiary ekranu	Min 180 x 180 cm
Format	1:1
Przekątna obrazu	Min 97 [cale]
Wymiary obrazu	Min 175 x 175 cm
Przekrój kasety	Max ø6.5 cm
Materiał obudowy	stal
Rodzaj powierzchni	Matt White
Waga netto	Max 7.8 kg

15.) Sieć bezprzewodowa w pracowni komputerowej w Szkole Podstawowej nr 3 - 1szt

Podstawowe założenia: wszystkie prace należy wykonać w oparciu o obowiązujące przepisy i zasady określone w PN-EN 50173-1

Zamawiający zaleca przeprowadzenie wizji technicznej przed złożeniem oferty celem dokładnego oszacowania ilości materiałów niezbędnych do wykonania zadania oraz dokonania niezbędnych uzgodnień.

Wszelkie usterki wynikłe podczas prowadzenia prac przy modernizacji i rozbudowie Wykonawca przywróci do stanu pierwotnego na własny koszt

W ramach budowy sieci bezprzewodowej Wykonawca dostarczy jeden serwer, zainstaluje i skonfiguruje go do prawidłowego działania w tym zapewni mechanizm tworzenia kopii zapasowych ważnych danych Oprogramowanie serwera ma posiadać możliwość pracy jako kontroler domeny. Zarządzanie użytkownikami domeny, tworzenie kopii zapasowych ich plików, modyfikacja praw dostępu do danych i aplikacji dostępnych dla użytkowników ma się odbywać centralnie na serwerze. Użytkownicy logujący się do serwera mają możliwość umieszczania własnych danych na dyskach sieciowych przypisanych do ich konta, oraz na ogólnodostępnym dysku sieciowym. Serwer ma posiadać funkcję udostępniania drukarki w sieci lokalnej

Okablowanie: trasy prowadzenia okablowania poziomego jak i pionowego należy skoordynować z istniejącymi instalacjami w budynku m.in. instalacją elektryczną, instalacją centralnego ogrzewania, wody, gazu, itp.

- prace należy prowadzić w czasie niekolidującym z przeprowadzaniem zajęć lekcyjnych
- na terenie szkoły przewiduje się jeden punkt dystrybucyjny PD do którego należy doprowadzić przyłącz z istniejącego łącza internetowego.

Wyposażenie PD

- szafa rack 6U
- patch panel 2x24
- przełącznik sieciowy 8p PoE
- kontroler WiFi
- listwę zasilającą
- przełącznik sieciowy 2x24 p

Zamawiający wymaga zainstalowania na terenie swojego obiektu 8 Access Point

Wykonawca przedstawi Zamawiającemu planowanie radiowe zasięgu sieci WiFi z graficznym pokryciem obszaru zaprojektowanych urządzeń na podkładzie (rzucie) przekazanym od Zamawiającego.

urządzenia zasilane w technologii PoE

standard sieci 802.11 b/g/n

częstotliwość WiFi 2.4GHz

szyfrowanie: WPA2, WPA, 64/128 bit WEP

dostęp do sieci wymaga autoryzacji

poprzez utworzenie segmentów VLAN należy wydzielić odrębne sieci w uzgodnieniu z Zamawiającym.

Charakterystyka urządzeń:

SERWER	
Parametr	**Charakterystyka**
Płyta główna	Serwerowa, jednoprocesorowa z możliwością instalacji modułu TPM

Procesor	Jeden procesor przynajmniej 4-rdzeniowy taktowany zegarem minimum 2,26 GHz posiadający pamięć podręczną cache o wielkości przynajmniej 8MB.
Zarządzanie	Zintegrowany moduł zarządzający z dedykowanym portem RJ45 i pełnym przekierowaniem konsoli KVM
Złącza kart rozszerzeń	Minimum 1x PCI-E 3.0 x8 (x16 slot), 1x PCI-E 3.0 x8 oraz 1x PCI-E 3.0 x4 (x8 slot)
Pamięć	Co najmniej 8GB RAM, możliwość rozbudowy do 64GB,
Karta sieciowa	Dwa porty 1Gb Ethernet (niezależne od karty zarządzającej), obsługa startu z iSCSI oraz PXE
Karta graficzna	Zintegrowana z płytą główną
Kontroler RAID	Zintegrowany z płytą główną kontroler SATA RAID 0,1,10, posiadający co najmniej sześć złącz SATA 6Gbps
Dysk twardy	Dwa dyski SSD przeznaczone do pracy ciągłej w serwerach, każdy o pojemności co najmniej 240GB oraz MTBF co najmniej 2mln godzin. Dwa dyski twarde przeznaczone do pracy ciągłej w serwerach, każdy o pojemności co najmniej 1TB i 64MB pamięci Cache.
Obudowa	Obudowa Tower. Minimum cztery wewnętrzne zatoki 3,5" umożliwiające beznarzędziowy montaż dysków twardych. Jeden zasilacz o mocy co najmniej 350W
Porty	Na przednim panelu: 2 x USB, na tylnym panelu: 1 x RS-232, 2 x USB 3.0, 1 x VGA, 2x RJ45. Wewnątrz serwera co najmniej jedno złącze USB 3.0 Typ A.
Certyfikaty	Certyfikat PN-EN ISO 9001:2001(ISO 9001:2001) na procesy projektowania, produkcję, sprzedaż i serwis, PN-EN ISO14001:2005 (ISO 14001:2005) oraz PN-ISO/IEC 27001:2007 lub nowsze Deklaracja producenta o zgodności z dyrektywami LVD 2006/95/WE oraz Dyrektywy EMC 2004/108/WE. Deklaracja producenta sprzętu o zgodności oferowanego serwera z wymaganiami normy Energy Star 2.0. Wymagane potwierdzenie obecności oferowanego modelu na stronie internetowej Energy Star przez dostarczenie wydruku ze strony http://www.eu-energystar.org z kategorii Enterprise server.
Wsparcie techniczne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego.
Oprogramowanie	Oprogramowanie serwera ma posiadać możliwość pracy jako kontroler domeny. Zarządzanie użytkownikami domeny, tworzenie kopii zapasowych ich plików, modyfikacja praw dostępu do danych i aplikacji dostępnych dla użytkowników ma się odbywać centralnie na serwerze. Użytkownicy logujący się do serwera mają możliwość umieszczania własnych danych na dyskach sieciowych przypisanych do ich konta, oraz na ogólnodostępnym dysku sieciowym. Serwer ma posiadać funkcję udostępniania drukarki w sieci lokalnej.

Monitor do serwera	
Parametr	**Opis**
Przekątna ekranu	Min 21,5 cali
Zalecana rozdzielczość obraz	Min 1920 x 1080 pikseli
Czas reakcji matrycy	Min 5 ms
Jasność	Min 200 cd/m2
Kąt widzenia poziomy	Min 90 stopni
Kąt widzenia pionowy	Min 65 stopni

Pobór mocy (praca/spoczynek)	Min 19/0,5 Wat
Montaż na ścianie (VESA)	Min 100 x 100 mm

SZAFA RACK	
Parametr	**Opis**
Kolor	RAL9004 Czarny
Masa netto:	max 21. kg
Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją	
przepusty kablowe	min. jeden w suficie, drugi w podłodze
Wymiary:	450 mm x 600 mm x 638 mm
Wysokość wewnętrzna:	12U

PRZEŁĄCZNIK SIECIOWY	
Parametr	**Opis**
liczba portów 1000 Mbit	Min 24 szt.
typ	zarządzany
przeznaczenie	do szaf RACK 19"
obsługiwane protokoły	IEEE 802.3u, IEEE 802.3i, IEEE 802.3ab, IEEE 802.3, IEEE 802.1Q, IEEE 802.1p
rozmiar tablicy adresów MAC	Min 8000
algorytm przełączania	store-and-forward
prędkość magistrali wew.	Min 48 Gb/s
obsługa VLANów	
Wymiary	Max 294 mmx 45mm x 180 mm

ROUTER WiFi	
Parametr	**Charakterystyka**
Porty:	min 4 x LAN100/1000Mb/s , 1x WAN 100/1000Mb/s 1x USB 3.0 1x USB 2.0
Przycisk:	WPS/RESET, Wyłącznik, wyłącznik sieci WiFI
Antena:	Antena: możliwość podłączenia 3 dwupasmowych anten zewnętrznych
Wymiary:	max222 x 87 x 169mm
Częstotliwość pracy:	min 2,4GHz oraz 5GHz
Standardy bezprzewodowe:	IEEE 802.11ac/n/a 5GHz, IEEE 802.11b/g/n 2,4GHz
Czułość odbiornika 5GHz	11a 6Mb/s-96dBm, 11a 54Mb/s: -79dBm, 11ac HT20: -71dBm, 11ac HT40:
Czułość odbiornika 2,4 GHz	11g 54M: -77dBm 11n HT20: -74dBm 11n HT40: -72dBm
EIRP CE:	<20dBm(2,4GHz)<23dBm(5GHz)
Funkcje transmisji bezprzewodowej	WDS bridge, WMM, Statystyki transmisji bezprzewodowej
Bezpieczeństwo transmisji bezprzewodowej:	min WEP 64/128 bit, WPA /WPA2, szyfrowanie WPA-PSK/WPA2-PSK
Funkcja	Quality of Service WMM, Kontrola przepustowości
Sieć WAN Dynamiczne IP/Statyczne IP/PPPoE/	
PPTP(Dual Access)/L2TP(Dual Access)/BigPond	
Zarządzanie:	Kontrola dostępu, Zarządzanie lokalne, Zarządzanie zdalne

DHCP:	Serwer, Klient, Lista klientów DHCP, Rezerwacja adresów
Przekierowanie portów:	Serwery wirtualne, Port Triggering, DMZ, UPnP
Kontrola dostępu :	Kontrola rodzicielska, lokalna kontrola dostępu do panelu zarządzania, lista hostów, harmonogram dostępu, zarządzanie regułami
Zabezpieczenia zapory sieciowej:	Ochrona przed atakami DoS, zapora sieciowa SPI, filtrowanie domen, adresów IP i MAC, wiązanie adresów IP i MAC
Protokoły:	IPv4 oraz IPv6
Udostępnianie urządzeń USB	Serwer Samba(udostępnianie dysków)/Serwer FTP/Serwer multimediów/Serwer druku
Funkcja Guest Network Jedna sieć dla gości w paśmie 2,4GHz	
Jedna sieć dla gości w paśmie 5GHz	
Wymagania systemowe	Microsoft Windows 98SE, NT, 2000, XP, Vista™ lub Windows 7, Windows 8, MAC OS, NetWare, UNIX lub Linux
Zestaw powinien zawierać	min 3 anteny, Instrukcja szybkiej instalacji, Płyta CD, Zasilacz 12V

PRZEŁĄCZNIK SIECIOWY PoE	
Parametr	**Opis**
Zasilanie	230V Wyjścia POE 22-24VDC (max 18W/port)
Liczba portów	min. 1 port 10/100Mbps min. 8 portów 10/100/1000Mbps min. 1 port USB
Liczba portów obsługujących POE	min. 8
Zarządzanie	przez przeglądarkę internetową
Obudowa	w części wykonana z metalu
Optyczna sygnalizacja pracy	Zasilanie switch'a; Link/Act; PoE Status
Zasilanie	230V Wyjścia POE 22-24VDC (max 18W/port)

ACCESS POINT	
Parametr	**Opis**
Częstotliwość	2,4 GHz
Praca w standardzie	802.11 b/g/n
Zasilanie	PoE
wymiary	max: 201x201x37mm
Montaż	Ściana, sufit
Porty	min 1x Ethernet 10/100
Bezpieczeństwo	WEP,WPA-PSK,WPA-TKIP,WPA2-AES
Wskaźnik zasilania	LED
Antena	2x2MIMO
Zużycie mocy	Max 4.1 W
Konfiguracja	Przeglądarka WWW, dedykowany kontroler

KONTROLER	
Parametr	**Opis**
Pojemność dysku	Min 0.1 TB

wewnętrznego	
Łączność	LAN (10,100,1000 Mbit/s), USB
Napięcie wyjściowe adaptera AC	Min 5 V
Wymiary	Max 21,8x44x122
Waga	112g
W zestawie znajduje się zasilacz oraz karta micro-SD o pojemności min. 16GB	

16.) Kserokopiarka A3 kolor – 2szt

Parametr	Opis
Pojemność wejściowa	Podajnik 1: 300 arkuszy
Podajnik uniwersalny	100 arkuszy
Rozdzielczość skanowania	min 600 x 600 dpi
Rozdzielczość kopiowania	min 600 x 1200 dpi
Format oryginalny	A3, A4, A5, A6, B4, B5, Letter, Legal 13, Legal 13.5, Legal 14, Executive, Tabloid (11" x 17"), Statement, Folio, rozmiar niestandardowy
Format papieru do kopiowania	A3, A4, A5, A6, B4, B5, B6, Letter, Legal 13, Legal 13.5, Legal 14, Executive, Tabloid (11" x 17"), Statement, Folio, 8K, 16K, koperty,
Skalowanie kopiowania	min25-400%
Panel sterowania	Ekran dotykowy LCD 7-calowy (17,5cm) podświetlany kolorowy ekran dotykowy LCD i górne przyciski;
Szybkość kopiowania	min 23 kopii na minutę w formacie A4 w kolorze, 23 kopii na minutę w formacie A4 w czerni
Czas uzyskania pierwszej kopii	W kolorze: około 14,5 sekundy; w czerni: około 14,5 sekundy
Czas nagrzewania	Około 32,0 s od momentu włączenia
Zasilanie	220-240 V AC ±0%
Pobór mocy	Podczas pracy: max. 1 400W / Śr. 850W Tryb gotowości: max 120W
Pamięć (Std./Maks.)	min 1,2GB/1,2GB
Bezpieczeństwo i przepisy dotyczące środowiska	Blue Angel, Energy Star, Dyrektywa dotycząca kompatybilności elektromagnetycznej, Oznaczenie GS, Oznaczenie CE
Poziom hałasu	Podczas pracy: max 55 dBA
Podczas pracy	11-31°C, 21-79% wilgotność względna
Wymiary (wys. x szer. x głęb.)	max 564 x 601 x 701 mm
Waga (wraz z materiałami eksploatacyjnymi)	max 65,0 kg
Obciążalność max.	60 000 stron miesięcznie
DRUK Szybkość drukowania	min A4 23 str./min w kolorze, 23 str./min monochromatyczne A3 13 str./min w kolorze, 13 str./min monochromatyczne
Czas uzyskania pierwszej kopii	W kolorze: około 14,5 sekundy; w czerni: około 14,5 sekundy
Rozdzielczość druku	min 600 x 600 dpi 600 x 1200 dpi (4 poziomy)600 x 600 dpi
Fizyczna wielkość plamki	min 600 dpi
Interfejs	1000BASE-T/100BASE-TX/10BASE-T, USB 2.0 (High Speed), Host USB 2.0 (High Speed), Protokół
Język drukarki	Emulacja PostScript 3, emulacja PDF v1.7, emulacja PCL 5c, emulacja PCL 6 (XL), emulacja XPS, emulacja IBM ProPrinter, emulacja Epson FX
Obsługiwane systemy operacyjne	Windows 8.1, Windows 8.1 x64, Windows 8, Windows 8 x64, Windows 7, Windows 7 x64, Windows Vista, Windows Vista

	x64, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2008 x64, Windows Server 2003, Windows Server 2003 x64, Mac OS X 10.6, OS X 10.7, OS X 10.8, OS X 10.9, OS X 10.10,
Czcionka	Czcionki Adobe PostScript 80, 87 skalowalnych czcionek emulacji PCL, 4 czcionki bitmapowe
FAX Format papieru	min A3, A4, A5, A6, B4, B5, B6, Letter, Legal 13, Legal 13.5, Legal 14, Executive, Tabloid (11" x 17"), Statement, Folio, 8K, 16K, koperty, pocztówka, pocztówka zwrotna, rozmiar niestandardowy

17.) Ekran wielkoformatowy – 1szt

Parametr	Opis
Ekran	elektrycznie rozwijany
Format	16:10
Rozmiar powierzchni aktywnej	400x250
Szerokość całkowita ekranu z kasetą	409,6cm +/-2cm
Powierzchnia	Clear Vision
Obudowa	Aluminiowa, srebrny kolor
Przełącznik	ścienny natynkowy
Powierzchnia projekcyjna	Gain- 1,0 Kąt widzenia – 150° Grubość – 0,42mm
Wał nawojowy z wmontowanym cichym napędem rurowym	
Montaż	ścienny lub sufitowy
	Silnik (230V – 50Hz) wyposażony w elektryczne zabezpieczenie przypadkowego rozwinięcia ekranu
Silnik rurowy z termiczną krańcówką	
Silnik zamontowany wewnątrz kasety	
Połączenie	4 przewodowe o długości kabla 1,5m wychodzący z kasety, gotowe do podłączenia do zasilania
Kaseta	– anodowane aluminium
Przekrój kasety bez mocowania	min 17,7cm x 16,6cm