



Załącznik Nr 1 do SWZ - OPZ

OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

Zakup i wdrożenie rozwiązań zwiększających poziom bezpieczeństwa systemów informacyjnych i sieci teleinformatycznej Starostwa Powiatowego w Kielcach w ramach projektu „Poprawa poziomu cyberbezpieczeństwa Starostwa Powiatowego w Kielcach w ramach projektu grantowego CYBERBEZPIECZNY SAMORZĄD”, dofinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Część 1. Dostawa i wdrożenie niewygasających licencji na oprogramowanie poczty elektronicznej i pracy grupowej wraz ze wsparciem producenta do 30.06.2026 r. dla potrzeb Starostwa Powiatowego w Kielcach.

Część 2: Dostawa, wdrożenie, konfiguracji i instalacja komponentów sprzętowych i programowych, do budowy kompletnej infrastruktury sieci bezprzewodowej na potrzeby Starostwa Powiatowego w Kielcach.



Część 1: Dostawa i wdrożenie niewygasających licencji na oprogramowanie poczty elektronicznej i pracy grupowej wraz ze wsparciem producenta do 30.06.2026 r. dla potrzeb Starostwa Powiatowego w Kielcach.

I. Przedmiotem zamówienia jest:

1. Zakup i dostarczenie niewygasających licencji komercyjnych na oprogramowanie poczty elektronicznej i pracy grupowej wraz ze wsparciem producenta do 30.06.2026r.
2. Kompletnie wdrożenie rozwiązania na infrastrukturze Zamawiającego;
3. Wykonawca musi posiadać doświadczenie w realizacji co najmniej dwóch wdrożeń systemu poczty elektronicznej w środowiskach korporacyjnych lub jednostkach publicznych, obejmujących co najmniej 100 skrzynek pocztowych każde. Doświadczenie powinno obejmować pełen proces wdrożenia: migrację skrzynek, konfigurację systemu oraz wsparcie powdrożeniowe.
4. Wykonawca musi zapewnić, że wszystkie prace związane z migracją, konfiguracją i wdrożeniem systemu poczty elektronicznej będą wykonywane przez osoby posiadające odpowiednie kwalifikacje zawodowe tj. aktualne certyfikaty producenta potwierdzające kompetencje w zakresie administracji i obsługi systemu poczty elektronicznej, wydane przez producenta lub autoryzowanego partnera producenta, bądź równoważne certyfikaty uznawane w branży IT.
5. Migracja kont pocztowych wraz z danymi użytkowników z obecnego serwera pocztowego.
6. szkolenia administratorów

II. Wymagania techniczne system poczty elektronicznej:

1. Dostarczenie niewygasających licencji systemu dla 500 kont użytkowników ze wsparciem technicznym producenta zaoferowanego systemu. W ramach dostarczonych licencji konieczna jest możliwość podłączenia min. 500 klientów korzystających z urządzeń mobilnych oraz pakietu zawierającego oprogramowanie Microsoft Outlook 2016-2024 (szczegóły opisane w punkcie „Funkcjonalność zaawansowana”.
2. Zamawiający wymaga dostarczenia systemu poczty elektronicznej w wersji komercyjnej (enterprise), objętej odpłatną licencją producenta oraz aktywnym wsparciem technicznym producenta.
3. System nie może być oferowany wyłącznie w modelu open source ani w wersji pozbawionej komercyjnego wsparcia producenta.
4. Dostarczenie polskojęzycznej dokumentacji użytkownika końcowego w wersji filmów instruktażowych.
5. Przeprowadzenie szkolenia dla administratorów systemu w siedzibie Zamawiającego.
6. Dostarczenie polskojęzycznej dokumentacji powdrożeniowej.
7. Udzielenie asysty technicznej wdrażającego (Wykonawcy) do 30.06.2026r.

8. Wykonawca udzieli gwarancji na dostarczony i wdrożony system poczty elektronicznej na okres 24 miesiące od dnia podpisania protokołu odbioru końcowego, obejmującej prawidłowe działanie systemu oraz usuwanie błędów i usterek.

Serwer systemu poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

Funkcjonalności podstawowe:

- a) Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.
- b) Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
- c) Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
- d) Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
- e) Możliwość tworzenia zadania z wiadomości pocztowej z poziomu klienta w przeglądarce.
- f) Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości w standardzie SMIME.
- g) Obsługa innych aplikacji za pomocą interfejsów SOAP/REST/API poprzez udostępnianie usług (np. Web-services).
- h) Możliwość zablokowania przesłania i przekazywania wiadomości do domen zewnętrznych.
- i) System udostępnia API programistyczne za pomocą którego można integrować się z systemami trzecimi.
- j) Możliwość wykorzystania Microsoft Active Directory do uwierzytelniania użytkowników, prezentacji listy użytkowników w globalnej książce adresowej i SSO.
- k) Możliwość wykorzystania zewnętrznych katalogów LDAP do uwierzytelniania użytkowników i prezentacji listy użytkowników w globalnej książce adresowej.
- l) Możliwość podłączenia 500 użytkowników do serwera za pomocą klienta Web bądź innego oprogramowania opartego o standardowe protokoły IMAP, SMTP, CalDAV.
- m) System pocztowy musi być skalowalny do obsługi ponad 5000 kont użytkowników lub więcej, przy wykorzystaniu dodatkowego sprzętu, bez konieczności reinstalacji.
- n) System musi być zabezpieczony przed lukami bezpieczeństwa wynikającymi z technologii, w której został stworzony.

Funkcjonalność zaawansowana:

- a) Pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2016 i nowszych wersji oprogramowania MS Outlook od 2016 do 2024.
- b) System posiada mechanizm wymuszenia polityk zabezpieczeń na urządzeniach mobilnych z systemami Android, Windows Phone i iOS. Polityki powinny wymuszać zdefiniowane hasła, czy jego złożoność, czy też możliwość szyfrowania pamięci urządzenia i kart pamięci.

- c) Panel webowy musi spełniać zasady tworzenia responsywnych aplikacji webowych, zapewniając użytkownikom spójne wrażenia i pełną funkcjonalność na wszystkich urządzeniach (desktop, tablet, smartfon).
- d) Panel webowy musi być skonstruowany jako progresywna aplikacja internetowa (PWA) uruchamiana tak jak zwykła strona internetowa, ale umożliwiającą stworzenie wrażenia działania jak natywna aplikacja mobilna lub aplikacja desktopowa. PWA może zostać zainstalowana, wtedy może posiadać własną ikonę na pulpicie oraz być niezależna od przeglądarki.
- e) Panel webowy musi posiadać możliwość integracji z rozwiązaniami ZOOM, SLACK, DROPBOX, ONEDRIVE, NEXTCLOUD.

Funkcjonalności pozostałe:

- a) Możliwość drukowania wiadomości oraz wyświetlania podglądu wydruku.
Możliwość wyboru i drukowania wielu wiadomości jednocześnie.
- b) Możliwość definiowania reguł filtrowania i priorytetów dla wiadomości przychodzących i wychodzących.
- c) Możliwość stosowania nowych reguł na istniejących wiadomościach.
- d) Możliwość definiowania własnego podpisu. Możliwość konfiguracji przez administratorów maksymalnej liczby znaków używanych w podpisach.
- e) Przeciągnięcie wybranej wiadomości do kalendarza powoduje automatyczne utworzenie terminu na podstawie tej wiadomości.
- f) Prezentowanie wiadomości poczty elektronicznej użytkownika z poziomu interfejsu webowego w widoku wg kolejności napływania lub grupującym w konwersacje.
- g) Możliwość zdefiniowania priorytetu wysyłanej wiadomości pocztowej.
- h) Możliwość załączania definiowalnej przez administratora liczby załączników do wysyłanej wiadomości elektronicznej o rozmiarze maksymalnym definiowalnym przez administratora
- i) Pobieranie dużej ilości załączników wiadomości elektronicznej w postaci jednej paczki (np. skompresowanego archiwum zip).
- j) Wyświetlanie bieżącej zajętości przestrzeni skrzynki użytkownika.
- k) Wyszukiwanie wiadomości wg zadanych kryteriów min.: adresu/nazwy nadawcy/odbiorcy, temacie wiadomości, dacie wysłania.
- l) Możliwość oznaczenia wiadomości flagą lub znacznikami definiowanymi przez użytkownika umożliwiającymi grupowanie szybsze wyszukiwanie wiadomości.
- m) Obsługa funkcjonalności drag&drop w interfejsie webowym w zakresie przenoszenia wiadomości pomiędzy folderami.
- n) Interfejs webowy do obsługi poczty powinien współpracować poprawnie z przeglądarkami internetowymi zarówno w systemach stacjonarnych jak i mobilnych
- o) Interfejs webowy powinien udostępniać tryb nowoczesny, który jest responsywny i reaktywny, dostosowujący się do urządzenia na którym wyświetlana jest ten interfejs, opierający się o nowoczesne frameworki, np. Preact, React, Vue.js
- p) Interfejs webowy do obsługi poczty powinien umożliwić użytkownikowi tworzenie wiadomości przez edytor WYSWIG z możliwością stosowania różnego rodzaju formatowań, krojów czcionek, stylów itp.
- q) Umożliwienie użytkownikowi wysyłanie wiadomości w formacie tekstowym lub HTML.
- r) Automatyczne podpowiadanie adresu odbiorcy z dostępnych książek adresowych podczas tworzenia wiadomości.
- s) Interfejs webowy do obsługi poczty powinien umożliwić użytkownikowi obsługę innych kont pocztowych poprzez protokół POP3 lub IMAP (funkcja nadawana użytkownikowi tylko przez administratora).
- t) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi

zdefiniowanie parametrów odpowiedzi automatycznej. Wymagane parametry autorespondera to czas działania, treść odpowiedzi, przekierowanie wiadomości na inny adres, itp.

- u) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi zdefiniowanie przekazywania wiadomości na inny adres poczty elektronicznej np. na czas jego nieobecności w pracy, urlopu. Definiowalne powinno być ograniczenie przesyłania tylko do własnej domeny.
- v) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi ustawienie żądania potwierdzenia odbioru wiadomości przez odbiorcę.
- w) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi zmianę hasła na żądanie oraz wg polityki złożoności zdefiniowanej przez administratora
- x) Możliwość zablokowania konta użytkownika po określonej liczbie nieudanych prób logowania w zadanym okresie czasu.
- y) Możliwość zdefiniowania podpisu użytkownika dołączanego automatycznie do każdej nowej wysyłanej wiadomości.
- z) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi eksport/import książki adresowej do pliku CSV.
- aa) Możliwość odzyskania skasowanej przez użytkownika wiadomości z folderu „kosz” z poziomu interfejsu webowego pracy grupowej.
- bb) Możliwość personalizacji wyglądu interfejsu webowego przez użytkownika poprzez dostępne w systemie pracy grupowej szablony wyglądu i kolorystyki, rodzaje czcionek oraz układy elementów widoku.

Funkcjonalności pozostałe zaawansowane:

- a) Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi dostęp do wiadomości przechowywanych w archiwum.
- b) Możliwość przeglądania wiadomości archiwalnych z oferowanego systemu do archiwizacji z poziomu interfejsu webowego pracy grupowej.
- c) System powinien być wyposażony w mechanizmy nadrzędne, pozwalające na automatyczną archiwizację wszystkich wiadomości wchodzących i wychodzących z konta użytkownika.

Konakty

- a) Możliwość prezentacji kontaktów jako listy.
- b) Możliwość importu, eksportu kontaktów z, do pliku .CSV, .VCF przez administratora lub użytkownika.
- c) Możliwość utworzenia przez użytkownika wielu książek adresowych w ramach jednego konta.
- d) Możliwość przenoszenia i kopiowania kontaktów pomiędzy książkami adresowymi (w oparciu o uprawnienia dostępu).
- e) Możliwość tworzenia przez użytkowników grup kontaktów.

Kalendarz

- a) Możliwość planowania spotkań i podglądu dostępności innych uczestników (wolny, zajęty).
- b) Możliwość zmiany przez użytkownika własnej informacji o dostępności.
- c) Możliwość tworzenia spotkań cyklicznych oraz wyjątków do spotkań cyklicznych.
- d) Możliwość rezerwacji zasobów (lokalizacja, wyposażenie, itp.) w ramach spotkania.
- e) Możliwość wyszukiwania dostępnych zasobów poprzez atrybuty (budynek, piętro, itp.).
- f) Możliwość włączenia alertu (pop-up) w związku ze zbliżającym się terminem.
- g) Możliwość prezentacji kalendarza w widokach: dzień, tydzień, miesiąc, dzień (godziny pracy), tydzień (godziny pracy).
- h) Możliwość konfiguracji godzin i dni roboczych.
- i) Możliwość tworzenia spotkania we wszystkich widokach kalendarza.
- j) Możliwość szybkiego akceptowania lub odrzucania terminu.
- j) Możliwość włączenia lub wyłączenia przez użytkownika automatycznych powiadomień e-mail na temat spotkań.

- k) Możliwość tworzenia przez użytkownika wielu kalendarzy w ramach jednego konta.
- l) Możliwość wyświetlania przez użytkownika wielu kalendarzy nakładanych w tym samym miejscu. Każdy kalendarz reprezentowany jest przez inny kolor.
- m) Możliwość oznaczenia terminów jako publiczne i prywatne.
- n) Możliwość publicznego udostępniania kalendarzy w trybie do odczytu.

Zadania

- a) Możliwość definiowania zadań, ustanowienia daty rozpoczęcia, priorytetu, śledzenia postępu i skuteczności wykonania zadania.
- b) Możliwość współdzielenia zadań z użytkownikami wewnętrznymi i zewnętrznymi wraz z ustanowieniem odpowiednich uprawnień (odczyt, zapis).
- c) Możliwość dołączania załączników (plików) do poszczególnych zadań.
- d) Możliwość synchronizacji zadań, kalendarza, kontaktów na systemach Windows (np. iCAL).
- e) Możliwość sortowania zadań (np.: Status, Data).

Pliki

- a) Możliwość przechowywania plików, kategoryzacji, podglądania ich zawartości w panelu webowym
- b) Możliwość wersjonowania plików.
- c) Możliwość tworzenia folderów w których umieszczane są pliki.
- d) Możliwość współdzielenia folderów z plikami z użytkownikami wewnętrznymi i zewnętrznymi wraz z ustanowieniem odpowiednich uprawnień (odczyt, zapis).
- e) Możliwość zapisu załączników mailowych w folderze plikowym.

Wyszukiwanie

- a) Możliwość szybkiego i efektywnego wyszukiwania. Indeksowanie zawartości skrzynki pocztowej po stronie serwera.
- b) Interfejs do obsługi konstrukcji zapytań zaawansowanych.
- c) Możliwość wyszukiwania dla danego typu elementu (poczty, kontaktów, dokumentów, itp.) lub przez typy elementów.
- d) Możliwość wyszukiwania obiektów zawierających: specyficzne słowa kluczowe, utworzonych w określonym okresie czasowym, zawierających załączniki, zawierających załączniki określonego typu, umieszczonych w określonych folderach, w oparciu o rozmiar obiektu, w oparciu o status przeczytany, nieprzeczytany, wysłanych do określonych adresatów, otrzymanych od określonych nadawców, w oparciu o temat, odebranych lub wysłanych z określonej domeny, kontaktów w udostępnionych książkach adresowych, zawartości wewnątrz załączników, terminów w kalendarzach, możliwość wyłączenia przez administratorów indeksowania wiadomości śmieci, wyszukiwania udostępnionych folderów.

III. Wymagania funkcjonalne przeglądarkowego klienta pocztowego:

1. Funkcje klienta przeglądarkowego:

- 1.1 Aplikacja Web (klient Web) musi być kompatybilna z następującymi przeglądarkami internetowymi:
 - a) Mozilla Firefox w najnowszej dostępnej wersji na dzień składania ofert.
 - b) Microsoft w najnowszej dostępnej wersji na dzień składania ofert.
 - c) Google Chrome w najnowszej dostępnej wersji na dzień składania ofert.
 - d) Apple Safari w najnowszej dostępnej wersji na dzień składania ofert.
- 1.2 Wszystkie elementy aplikacji muszą posiadać interfejs w języku polskim. Jako element interfejsu, Zamawiający określa również elementy konfiguracji poszczególnych części składowych systemu. W języku polskim są również wyświetlane wszystkie komunikaty przekazywane przez system, włącznie z

- komunikatami o błędach.
- 1.3 Aplikacja musi dostosowywać rozmiar wszystkich okien do aktualnych ustawień rozdzielczości ekranu.
 - 1.4 Zamawiający wymaga, aby dane ze wszystkich formularzy aplikacji do systemu były przesyłane do serwera w postaci zaszyfrowanej (bezpieczny protokół HTTPS/SSL).
 - 1.5 Obsługa prostego przeszukiwania musi być oparta na słowach kluczowych z użyciem indeksowania po stronie serwera.
 - 1.6 Możliwość przesuwania dynamicznej liczby zaznaczonych obiektów (wiadomości e-mail, dokumenty, pliki, zadania, kontakty, itd.) metodą „przeciągnij i upuść”.
 - 1.7 Możliwość automatycznego uzupełniania kontaktów podczas tworzenia lub edycji wiadomości. Adresy powinny być pobierane z zewnętrznej lub wewnętrznej, globalnej bazy adresowej lub bazy adresów użytkownika.
 - 1.8 Opcja sprawdzania i poprawiania pisowni w wiadomości e-mail, terminu kalendarza, dokumentów.
 - 1.9 Możliwość szybkiego wyświetlania załączników pakietu MS Office oraz pdf w formacie HTML.
 - 1.10 Automatyczne grupowanie wiadomości e-mail w wątku, umożliwiające sprawną organizację wiadomości. Wątki e-mail powinny być tworzone niezależnie od lokalizacji wiadomości (np. inny folder).
 - 1.11 Możliwość wykonywania operacji (tagowanie, przeciągnij i upuść, usuwanie, itp.) na wątkach wiadomości.
 - 1.12 Możliwość przeglądania treści zaznaczonej wiadomości w oknie odczytu.
 - 1.13 Możliwość tworzenia folderów osobistych oraz hierarchii folderów. Możliwość zdefiniowania czasu życia wiadomości w poszczególnych folderach w skrzynce pocztowej.
 - 1.14 Możliwość sortowania wiadomości na podstawie tematu, daty, nadawcy lub rozmiaru wiadomości email.
 - 1.15 Możliwość szybkiej kategoryzacji wiadomości poprzez dodawanie tagów ze zdefiniowanymi przez użytkownika nazwami i kolorami.
 - 1.16 Możliwość definiowania przez użytkownika własnych wiadomości o nieobecności. Możliwość definiowania przez użytkownika autoodpowiedzi w zadanym przedziale czasowym.
 - 1.17 Możliwość automatycznego zapisu tworzonej wiadomości e-mail. Podczas tworzenia lub odczytywania wiadomości możliwość wyświetlania każdego obiektu w osobnej karcie (zakładce), użytkownik powinien mieć możliwość swobodnego poruszania się pomiędzy kartami (zakładkami).
 - 1.18 Możliwość włączenia przez użytkownika automatycznego przekierowania wiadomości przychodzącej na inny adres z możliwością zapisu kopii przekierowywanej wiadomości w podstawowej skrzynce odbiorczej. Możliwość włączenia szybkich powiadomień o otrzymaniu nowej poczty na inny adres e-mail.
 - 1.19 Opcja „Odpowiedz”, „Odpowiedz wszystkim” z możliwością zachowania załączników z oryginalnej wiadomości.
 - 1.20 Możliwość wybrania wielu wiadomości i wykonania określonej operacji jak na jednej wiadomości np. oznaczenie jako przeczytane.
 - 1.21 Wizualizacja przyznanej pojemności konta oraz jej zużycia (za pomocą wskaźnika graficznego).
 - 1.22 Możliwość definiowania oraz zmiany przez użytkownika domyślnych preferencji okna odczytu wiadomości e-mail. Użytkownicy mogą ustawić czcionkę domyślną, rozmiar czcionki i kolor czcionki używany do tworzenia wiadomości e-mail oraz dokumentów
 - 1.23 Możliwość udostępniania przez użytkowników swoich folderów skrzynki pocztowej i ustanowienia poziomów uprawnień do zarządzania lub tylko do odczytu.
 - 1.24 Dostęp do wielu kont wewnętrznych dla uprawnionych użytkowników
 - 1.25 Możliwość definiowania przez użytkowników czarnych lub białych list e-mail.
 - 1.26 Możliwość importu, eksportu konta, kalendarza, kontaktów przez administratora lub użytkownika.



- 1.27 Możliwość przejścia klienta webowego w tryb offline dla przeglądarek Edge lub FireFox lub Chrome (bez podłączenia do serwera poczty).
- 1.28 Możliwość włączenia podwójnego uwierzytelniania użytkowników przy dostępie do usługi web za pomocą dodatkowego kodu pin generowanego z poziomu aplikacji mobilnej w trybie offline.

2. Funkcje pracy grupowej:

- 2.1 Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
- 2.2 Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
- 2.3 Mechanizm planowania spotkań z możliwością zapraszania uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
- 2.4 Możliwość udostępniania książek adresowych, zadań z możliwością definiowania poziomów dostępu do zadań, książek.
- 2.5 Mechanizm udostępniania współdzielonych skrzynek pocztowych.
- 2.6 Obsługa list i grup dystrybucyjnych.
- 2.7 Dostęp ze skrzynki do poczty elektronicznej.
- 2.8 Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności.
- 2.9 Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
- 2.10 Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.
- 2.11 Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych e-mail bez potrzeby wsparcia ze strony pracowników wydziału IT.
- 2.12 Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący priorytetyzacją wyników wyszukiwania.
- 2.13 System powinien umożliwiać użytkownikowi obsługę poczty elektronicznej poprzez przeglądarkę internetową jak również inne programy typu klient poczty e-mail
- 2.14 System powinien umożliwiać przesyłanie wiadomości pocztowych od adresatów zewnętrznych jak i wewnętrznych.
- 2.15 System powinien zapewnić dostęp do skrzynki pocztowej, kalendarza i książek adresowych również za pomocą urządzeń mobilnych obsługiwanych przez dostępne na rynku mobilne systemy operacyjne
- 2.16 System powinien pracować w oparciu o usługi katalogowe LDAP w którym przechowywane są dane konfiguracji usług i skrzynek użytkowników, a także umożliwiać integrację z zewnętrznym katalogiem LDAP,
- 2.17 Usługi katalogowe LDAP systemu muszą być zaimplementowane tak, aby nie było konieczności instalowania dodatkowego oprogramowania na urządzeniach klienckich użytkowników.
- 2.18 System powinien obsługiwać następujące protokoły: SMTP i SMTPS, POP3 i POP3S, IMAP i IMAPS, HTTP (redirect na HTTPS) i HTTPS, CalDAV, CardDAV
- 2.19 System powinien zapewnić w przypadku awarii pojedynczego serwera SMTP, transport elementem redundantnym (MTA, PROXY, itp.) do zewnętrznego serwera SMTP.
- 2.20 Możliwość zdefiniowania w systemie pracy grupowej, wielu domen pocztowych i prowadzenia dla nich kont użytkowników.

3. Wsparcie dla użytkowników mobilnych (funkcjonalność zaawansowana):

- 3.1 Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu.
- 3.2 Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem.
- 3.3 System musi zapewniać możliwość korzystania z usług systemu pocztowego (synchronizacja z serwerem) w tym kalendarzy, poczty, zadań, kontaktów przy pomocy urządzeń mobilnych typu PDA, SmartPhone, laptop, tablet pracujących na systemach mobilnych w tym: iOS, Android, Windows Mobile.
- 3.4 Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet - z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.
- 3.5 Możliwość synchronizacji automatycznej poczty, zadań, kalendarza i książki adresowej pomiędzy mobilnym klientem pocztowym a serwerem co najmniej dla 500 użytkowników.

4. Funkcjonalność klienta offline:

4.1 Możliwość współpracy z programem Microsoft Outlook w wersjach 2016, 2019, 2021, 2024 zapewniająca dwustronną synchronizację poczty, kontaktów i kalendarza między programem Microsoft Outlook, a serwerem.

4.2 Możliwość przechowywania wiadomości w programie Microsoft Outlook w trybie offline.

Możliwość automatycznej konfiguracji i dostępu do globalnej książki adresowej pomiędzy programem Microsoft Outlook a serwerem.

4.3 Możliwość bezpiecznego połączenia przez HTTPS, szyfrowanie całego ruchu między programem Microsoft Outlook a serwerem.

4.4 Możliwość udostępnienia kalendarza wraz z odpowiednimi uprawnieniami, za pomocą programu Microsoft Outlook wraz z podglądem wolny/zajęty dla innych użytkowników systemu oraz podłączenia w swoim widoku kalendarzy udostępnionych przez innych.

4.5 Możliwość udostępnienia folderu pocztowego innym użytkownikom systemu oraz podłączenia w swoim widoku udostępnionych przez innych użytkowników folderów pocztowych.

4.6 Możliwość synchronizacji zadań utworzonych w programie Microsoft Outlook.

4.7 Możliwość synchronizacji kontaktów utworzonych w programie Microsoft Outlook

4.8 Możliwość dodawania stopek adresowych i ich synchronizacja z serwerem.

4.9 Możliwość pobierania z serwera tylko nagłówka wiadomości.

4.10 Automatyczne wykrywanie stanu połączenia online/offline bez konieczności ingerencji użytkownika w zmianę statusu.

4.11 Możliwość automatycznej, dwukierunkowej synchronizacji kategorii (tagów)

wiadomości między programem Microsoft Outlook, a serwerem.

- 4.12 Możliwość automatycznego opóźniania wysłania wiadomości ze skrzynki użytkownika
- 4.13 Możliwość ustawienia i synchronizacji z serwerem informacji o nieobecności.
- 4.14 Możliwość sprawdzenia pojemności skrzynki oraz jej zajętości na serwerze z poziomu programu Outlook.
- 4.15 Możliwość dodania pełnomocników, czyli osób, które mogą wysyłać pocztę „w imieniu” lub „jako” użytkownik. Synchronizacja tej informacji z serwerem.
- 4.16 Możliwość dodanie, edycji i synchronizacji z serwerem reguł poczty pozwalające na różne operacje na przychodzących mailach (np. przenieś do folderu, oznacz wiadomość, prześlij ją dalej), na podstawie ustawionych filtrów (np. temat, pole DO, DW).
- 4.17 Wsparcie mechanizmu podwójnej autentykacji 2FA uruchomionej na serwerze poczty dla Microsoft Outlook w wersjach 2016, 2019, 2021, 2024.

5 Zarządzanie i bezpieczeństwo systemu:

- 5.1 Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk.
- 5.2 Definiowanie rozmiaru skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu.
- 5.3 Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników.
- 5.4 Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer.
- 5.5 Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań - na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych - bez przyznawania pełnych uprawnień administracyjnych.
- 5.6 Wiadomości oznaczone przez użytkowników jako SPAM lub NIE SPAM są automatycznie dodawane do silnika szkolenia antyspamowego.
- 5.7 Możliwość blokowania załączników na podstawie takich kryteriów jak: rodzaj i rozmiar załączników.
- 5.8 Wsparcie dla technologii hierarchicznego przechowywania danych, czyli umożliwiającej przeniesienie danych użytkownika z zasobów szybkich na wolniejszy storage po spełnieniu warunku czasowego.
- 5.9 Możliwość zainstalowania i zarządzania certyfikatami z konsoli administracyjnej.
- 5.10 Możliwość tworzenia/planowania backupu środowiska oprogramowania.
- 5.11 Możliwość realizowania kopii /odzyskiwania pojedynczej skrzynki lub zestawu skrzynek w sposób pozwalający na zachowanie dostępności i ciągłości pracy.
- 5.12 Umożliwienie przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie - nawet w godzinach pracy biurowej bez zakłócenia pracy użytkowników.

6 Funkcje organizacji danych

- 6.1 Możliwość definiowania zasad przechowywania: wszystkich wiadomości, wiadomości śmieci, wiadomości do odzyskania oraz wiadomości usuniętych.
- 6.2 Możliwość przeniesienia skrzynki pocztowej lub pocztowych z jednego serwera na drugi bez konieczności przestoju systemu lub generowania zdarzeń mających wpływ na działanie innych skrzynek.
- 6.3 Możliwość włączenia funkcji odzyskiwania przez użytkownika usuniętych elementów, w określonym przez administratora systemu czasie.

7 Funkcje administracji systemem

- 7.1 Możliwość administracji systemem przez interfejs przeglądarkowy i klasyczną linię komend (Command Line Interface).
- 7.2 Możliwość tworzenia i zarządzania wieloma domenami w ramach jednej instancji serwera.
- 7.3 Możliwość korzystania z różnych globalnych list adresowych dla każdej z domen.
- 7.4 Możliwość przyznania określonej przestrzeni dyskowej dla określonej domeny.
- 7.5 Możliwość przyznania określonej przestrzeni dyskowej dla określonego konta.
- 7.6 Możliwość przeniesienia domeny.
- 7.7 Możliwość przeszukiwania skrzynek pocztowych z poziomu konsoli administracyjnej na podstawie kwerendy wyszukiwania, z możliwością wybrania wszystkich lub tylko grupy kont pocztowych do przeszukania. Wyniki zapisywane są jako kopie wiadomości, na zdefiniowanej w zapytaniu skrzynce pocztowej, w wybranym folderze docelowym. System musi umożliwiać nadawanie uprawnień do przeszukiwania treści skrzynek dla wybranych użytkowników.
- 7.8 Możliwość przypisania użytkownikowi zastępczego adresu e-mail (aliasu).
- 7.9 Możliwość tworzenia grup dystrybucyjnych wiadomości e-mail.

8 Funkcje edycji dokumentów

- 8.1 System powinien mieć możliwość edycji dokumentów Office: dokument tekstowy, arkusz kalkulacyjny, prezentacja.
- 8.2 Moduł edycji dokumentów jest dostępny w panelu webowym i pozwala na edycję dokumentów już zapisanych i tworzenie nowych, zapisywanych w folderach plikowych.
- 8.3 Moduł powinien mieć wsparcie minimum dla podstawowych formatów MSOffice: .doc, .xls i .ppt

9 Funkcje archiwum pocztowego

- 9.1 Archiwum pocztowe musi umożliwiać realizację polityk składowania i dostępu do danych archiwalnych w dwóch wariantach:
 - a) W archiwum są umieszczone wszystkie dane poczty przychodzącej/wychodzącej wraz z załącznikami.
 - b) Każdy użytkownik systemu za pomocą panelu web interfejsu systemu poczty elektronicznej może samodzielnie wykonać operację przeniesienia jednej bądź wielu wiadomości do systemu archiwum z możliwością pozostawienia wiadomości na swoim profilu bądź jej skasowania po przesłaniu do archiwum.
- 9.2 Użytkownik systemu może w panelu web interfejsu poczty wskazać samodzielnie, czy poczta ma być archiwizowana automatycznie i jak ma działać mechanizm kwalifikacji (data) wiadomości do automatycznej archiwizacji.
- 9.3 System archiwizacji poczty musi posiadać dedykowany panel web dla użytkowników systemu, w którym mogą oni wykonać operacje: filtrowania wiadomości, oznaczania ich tagami, przesłania wiadomości do swojego konta pocztowego.
- 9.4 System archiwizacji poczty musi posiadać dedykowany interfejs administratora umożliwiający:
 - a) tworzenie użytkowników
 - b) tworzenie grup
 - c) dodawanie domen
 - d) tworzenie zasad archiwizacji
 - e) tworzenie zasad retencji
 - f) tworzenie schematów wyszukiwania automatycznego
 - g) przeglądanie statystyk archiwum
 - h) informacje na temat stanu systemu
 - i) audyt (informacje na temat operacji jakie użytkownicy wykonywali w systemie)
- 9.5 Możliwości konfiguracyjne systemu archiwizacji:
 - a) Integracja z AD.
 - b) Logowanie użytkowników na podstawie danych z domeny LDAP Zimbra, Exchange, Lotus, etc.
 - c) Integracja przy wykorzystaniu IMAP.

- d) Logowanie poprzez autentykację IMAP na głównym serwerze pocztowym.
- e) Przywracanie poczty przy wykorzystaniu protokołu IMAP.
- f) Integracja przy wykorzystaniu POP3.
- g) Logowanie poprzez autentykację POP3 na głównym serwerze pocztowym.
- h) Integracja z google authenticator.
- i) Pełna integracja archiwum pocztowego z oferowanym systemem poczty i pracy grupowej.
- j) 3 tryby archiwizacji poczty: manualny, użytkownika i zaplanowany.
- k) Elastyczna konfiguracja na poziomie: użytkownika, klasy usług oraz administratora.
- l) Zintegrowane zarządzanie archiwum z panelem administracyjnym systemu poczty i pracy grupowej.
- m) Dedykowana zakładka archiwum w panelu WWW użytkownika.
- n) Obsługa SSO pomiędzy serwerem archiwum a serwerem poczty).
- o) Raporty o stanie zrealizowanych zadań archiwizacji dla administratora.
- p) Podgląd zrealizowanych zadań archiwizacji dla użytkownika (online).
- q) Wsparcie dla instalacji wieloserwerowych.
- r) Możliwość włączenia/wyłączenia kosza użytkownika z obsługi archiwum.
- s) Możliwość ustawienia daty ograniczającej dostęp użytkownika do danych archiwalnych poczty.

Funkcjonalność archiwum pocztowego ma być dostępna przez okres minimum 24 miesięcy.

10 Archiwizacja wiadomości

- 10.1 Oprogramowanie musi zawierać moduł archiwalny oferujący możliwość wyszukiwania wiadomości po ich treści oraz załącznikach, sortowanie według zadanego klucza oraz konfigurowanie polityki retencji dla minimum 500 kont.
- 10.2 Interfejs webowy do obsługi poczty powinien umożliwiać użytkownikowi dostęp do wiadomości przechowywanych w archiwum za zgodą administratora systemu.
- 10.3 System powinien być wyposażony w mechanizmy nadrzędne, pozwalające na włączenie automatycznej archiwizacji wszystkich wiadomości wchodzących i wychodzących dla jednego lub wielu kont. Minimum dla 500 kont.
- 10.4 Mechanizm Archiwum musi umożliwiać wyszukiwanie wiadomości e-mail w aktywnych i zarchiwizowanych skrzynkach pocztowych oraz kopiowanie wyników do określonej skrzynki pocztowej.
- 10.5 Oprogramowanie musi zawierać moduł archiwalny oferujący możliwość wyszukiwania wiadomości po ich treści oraz załącznikach, sortowanie według zadanego klucza oraz konfigurowanie polityki retencji.

11 Zdolność do integracji

- 11.1 System musi zapewnić możliwość rozszerzania funkcjonalności poprzez dodatkowe moduły (zarówno od strony interfejsu użytkownika, jak i administratora - frontend):
- 11.2 W szczególności system musi zapewnić możliwość rozszerzenia i pełnej integracji w warstwie serwerowej (backend).
- 11.3 W szczególności system musi zapewnić możliwość rozszerzenia i pełnej integracji w warstwie interfejsu użytkowników oraz administratorów (frontend) poprzez moduły instalowane przez interfejs administratora.
- 11.4 Producent musi zapewnić dokumentację tworzenia dodatkowych modułów rozszerzających zarówno warstwę frontend i backend.
- 11.5 Moduły warstwy UI muszą mieć możliwość instalacji z poziomu panelu administratora.

12 Szkolenie administracyjne

Kurs w formie warsztatowej obejmujący zagadnienia związane z tematem instalacji, zarządzania i prac konserwacyjnych dla oferowanego systemu.
Kurs szkoleniowy musi obejmować minimum:

1. Przeszkolenie z architektury systemu.
2. Wdrożenie w proces instalacji systemu.
3. Rozwiązywanie problemów podczas instalacji.
4. Obsługa konsoli administracyjnej.
5. Korzystanie z narzędzi CLI.
6. Korzystanie z narzędzi służących do monitoringu systemu, logów systemowych.
7. Realizacja polityki backupu.
8. Korzystanie z podpowiedzi w systemie.
9. Zagadnienia związane z migracją kont pocztowych.
10. Zabezpieczenia systemu AV/AS.
11. Integracja usług Active Directory.
12. Konfiguracji i administrowania systemem archiwum pocztowego.
 - Czas trwania szkolenia: 4 dni –min.28 godzin zegarowych.
 - Ilość administratorów do przeszkolenia: 5 osoby.
 - Zamawiający wymaga, aby szkolenie z obsługi systemu poczty elektronicznej było prowadzone przez osobę posiadającą aktualny certyfikat potwierdzający kwalifikacje w zakresie administracji i obsługi tego systemu, wydany przez producenta lub autoryzowanego partnera producenta, oraz posiada udokumentowane min. 2 szkolenia z tego zakresu.
 - Materiały szkoleniowe: każdy z uczestników otrzyma materiały szkoleniowe w formie elektronicznej.
 - Miejsce szkolenia: w siedzibie Zamawiającego lub zdalnie.

13 Support producenta systemu

- 13.1 Należy wskazać link do strony producenta opisujący:
 - a) Poziomy wsparcia definiujące szczegółowe warunki dla oferowanej wersji wsparcia.
 - b) Czas reakcji na zgłoszenie (SLA).
 - c) Link do strony obsługi klienta (Customer Support Portal), umożliwiającej zalogowanie się na indywidualne konto supportowe klienta.

Część 2: Dostawa, wdrożenie, konfiguracji i instalacja komponentów sprzętowych i programowych, do budowy kompletnej infrastruktury sieci bezprzewodowej na potrzeby Starostwa Powiatowego w Kielcach.

Zamówienie obejmuje dostawę, wdrożenie, konfigurację i instalację komponentów sprzętowych i programowych, do budowy kompletnej infrastruktury sieci bezprzewodowej, zgodnie z poniższym opisem. W ramach zamówienia, dostawca jest zobowiązany do dostarczenia urządzeń klasy Access Point w 3 konfiguracjach, zgodnie z poniższym opisem zawartym w tabelach. Dokument zawiera również opis usług związanych z dostawą, instalacją i konfiguracją dostarczonych komponentów.

Zestawienie ilościowe urządzeń klasy Access point:

1. Access Point konfiguracja 1 – 40 szt.
2. Access Point konfiguracja 2 – 2 szt.
3. Access Point konfiguracja 3 – 2 szt.

Access Point, konfiguracja 1, ilość – 40 szt.

Lp.	Wymaganie	Opis warunków spełnienia wymagań
1.	Wymagania funkcjonalne	<ol style="list-style-type: none"> 1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. 2. Punkt dostępowy musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz (standard 802.11a/n/ac wave 2/ax) oraz 2.4GHz (standard 802.11b/g/n/ax). 3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: <ol style="list-style-type: none"> a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https. b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki. c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI oraz CLI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 4. Musi być zapewniona funkcja wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:



		<ol style="list-style-type: none">a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego.b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny.c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe.d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję.e. Wirtualny kontroler musi posiadać adres IP, za pomocą którego można zarządzać klastrem. Adres ten, w przypadku awarii musi podążać za nowym wirtualnym kontrolerem i pozostawać bez zmian.f. W ramach jednej grupy (klastra) musi być możliwe używanie Punktów Dostępowych różnego typu, np. w standardzie 802.11n i 802.11ac, które są zarządzane za pomocą tego samego wirtualnego kontrolera.g. Zamawiający wymaga, aby w ramach jednego klastra istniała możliwość pracy minimum 120 urządzeń . <ol style="list-style-type: none">5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.6. Punkt dostępowy musi mieć możliwość pracy jako analizator widma.7. W system operacyjny musi być wbudowana pełnostanowa zaporą sieciowa.8. W system musi być wbudowany serwer DHCP.9. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.10. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:<ol style="list-style-type: none">a. EAP-TLSb. PEAP-MSCHAPv2c. PEAP-GTCd. TTLS-MSCHAPv211. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP.12. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID.13. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
--	--	---

14. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
 - a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania.
 - b. Zewnętrzny portal WWW.
15. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
16. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
17. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
 - a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe.
 - b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu.
 - c. Rozkład ruchu pomiędzy różnymi punktami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma.
 - d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału.
 - e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz.
 - f. Wsparcie dla 802.11d oraz 802.11h.
 - g. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane.
18. Minimalizacja interferencji związanych z sieciami 3G/4G LTE.
19. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej.
20. Obsługa roamingu klientów w warstwie 2.
21. Obsługa monitoringu przez SNMP.
22. Obsługa logowania na zewnętrznym serwerze SYSLOG.
23. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
24. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
25. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
 - a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością.

		<ul style="list-style-type: none">b. Wykorzystanie pasma.c. Ilość klientów korzystających z systemu/interferujących.d. Ilość ramek wejściowych/wyjściowych dla każdego radia.e. Ilość odrzuconych /błędnych ramek/ dla każdego radia.f. Szum tła dla każdego radia.g. Wyświetlanie logów systemowych. <p>26. Punkt dostępowy musi posiadać 2 wbudowane anteny do pracy w trybie 2x2 MIMO o parametrach uzysku 4,9 dBi dla pasma 2,4 GHz oraz 5.7 dBi dla pasma 5 GHz.</p> <p>27. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2, 802.11ax</p> <p>28. Specyfikacja radia 802.11a/n/ac wave 2/ax:</p> <ul style="list-style-type: none">a. Obsługiwane częstotliwości:<ul style="list-style-type: none">- 5.150 ~ 5.250 GHz (low band)- 5.250 ~ 5.350 GHz (mid band)- 5.470 ~ 5.725 GHz (Europa)- 5.725 ~ 5.850 GHz (high band)b. Obsługa technologii OFDM i OFDMA.c. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.d. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm.e. Prędkości transmisji:<ul style="list-style-type: none">i. 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11aii. MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11niii. MCS0-MCS9, NSS = 1-2 (6.5 Mbps do 867 Mbps) dla 802.11aciv. MCS0-MCS11, NSS= 1-2 (3,6 Mbps do 867 Mbps dla 5 GHz) dla 802.11axf. Obsługa HT – kanały 20/40MHz dla 802.11n.g. Obsługa VHT – kanały 20/40/80MHz dla 802.11ac.h. Obsługa HE – kanały 20/40/80MHz dla 802.11ax.i. Wsparcie dla technologii DFS (Dynamic frequency selection).j. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac.k. Wsparcie dla:<ul style="list-style-type: none">i. MRC (Maximal ratio combining)ii. CDD/CSD (Cyclic delay/shift diversity)iii. STBC (Space-time block coding)iv. LDPC (Low-density parity check)v. Technologia TxBF
--	--	--

		<p>29. Specyfikacja radia 802.11b/g/n/ax:</p> <ul style="list-style-type: none">a. Częstotliwość 2,400 ~2,4835.b. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA.c. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256-QAM, 1024-QAM.d. Moc transmisji konfigurowalna przez administratora.e. Prędkości transmisji:<ul style="list-style-type: none">i. 1,2,5.5,11 Mbps dla 802.11bii. 6,9,12,18,24,36,48,54 Mbps dla 802.11giii. MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11niv. MCS0-MCS9, NSS= 1-2 (3,6 Mbps do 574 Mbps) dla 802.11ax <p>30. Punkt dostępowy musi posiadać co najmniej:</p> <ul style="list-style-type: none">a. 1 interfejs 100/1000Base-T:<ul style="list-style-type: none">i. z funkcją auto-sensing link oraz MDI/MDXii. z funkcją PoE/PoE+b. 1 interfejs konsolic. zasilanie zgodne z 802.3afd. przycisk przywracający konfigurację fabrycznąe. port USB 2.0f. slot zabezpieczający Kensington <p>31. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac/ax.</p> <p>32. Parametry pracy urządzenia:</p> <ul style="list-style-type: none">a. Temperatura otoczenia (zakres minimalny): 0-50 ° Cb. Wilgotność (zakres minimalny): 5% - 93%
2.	Pozostałe wymagania	<ul style="list-style-type: none">1. Punkty dostępowe muszą być objęte minimum 36-miesięczną gwarancją producenta. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 45 dni przesyła zamiennik.2. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.3. Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych4. Wszystkie urządzenia muszą być fabrycznie nowe.

Access Point, konfiguracja 2, 2 szt.

Lp.	Wymaganie	Opis warunków spełnienia wymagań
1.	Wymagania funkcjonalne	<ol style="list-style-type: none"> 1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. 2. Punkt dostępowy musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz (standard 802.11a/n/ac wave 2/ax) oraz 2.4GHz (standard 802.11b/g/n/ax). 3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: <ol style="list-style-type: none"> a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https. b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki. c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI oraz CLI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 4. Musi być zapewniona funkcja wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: <ol style="list-style-type: none"> a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego. b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny. c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe. d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję. e. Wirtualny kontroler musi posiadać adres IP, za pomocą którego można zarządzać klastrem. Adres ten, w przypadku awarii musi podążać za nowym wirtualnym kontrolerem i pozostawać bez zmian. f. W ramach jednej grupy (klastra) musi być możliwe używanie Punktów Dostępowych różnego typu, np. w standardzie 802.11n i 802.11ac, które są zarządzane za pomocą tego samego wirtualnego kontrolera. g. Zamawiający wymaga, aby w ramach jednego klastra istniała możliwość pracy minimum 120 urządzeń .



5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
6. Punkt dostępowy musi mieć możliwość pracy jako analizator widma.
7. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa.
8. W system musi być wbudowany serwer DHCP.
9. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
10. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
 - a. EAP-TLS
 - b. PEAP-MSCHAPv2
 - c. PEAP-GTC
 - d. TTLS-MSCHAPv2
11. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP.
12. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID.
13. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
14. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
 - a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania.
 - b. Zewnętrzny portal WWW.
15. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
16. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
17. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
 - a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe.
 - b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu.
 - c. Rozkład ruchu pomiędzy różnymi punktami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma.

		<ul style="list-style-type: none">d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału.e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz.f. Wsparcie dla 802.11d oraz 802.11h.g. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane. <p>18. Minimalizacja interferencji związanych z sieciami 3G/4G LTE.</p> <p>19. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej.</p> <p>20. Obsługa roamingu klientów w warstwie 2.</p> <p>21. Obsługa monitoringu przez SNMP.</p> <p>22. Obsługa logowania na zewnętrznym serwerze SYSLOG.</p> <p>23. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.</p> <p>24. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.</p> <p>25. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:</p> <ul style="list-style-type: none">a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością.b. Wykorzystanie pasma.c. Ilość klientów korzystających z systemu/interferujących.d. Ilość ramek wejściowych/wyjściowych dla każdego radia.e. Ilość odrzuconych /błędnych ramek/ dla każdego radia.f. Szum tła dla każdego radia.g. Wyświetlanie logów systemowych. <p>26. Punkt dostępowy musi posiadać 4 wbudowane anteny do pracy w trybie 4x4 MIMO o parametrach uzysku 3,5 dBi dla pasma 2,4 Ghz oraz 5,4 dBi dla pasma 5 GHz.</p> <p>27. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2, 802.11ax</p> <p>28. Specyfikacja radia 802.11a/n/ac wave 2/ax:</p> <ul style="list-style-type: none">a. Obsługiwane częstotliwości:<ul style="list-style-type: none">- 5.150 ~ 5.250 GHz (low band)- 5.250 ~ 5.350 GHz (mid band)- 5.470 ~ 5.725 GHz (Europa)- 5.725 ~ 5.850 GHz (high band)b. Obsługa technologii OFDM i OFDMA.
--	--	---

- c. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.
- d. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm.
- e. Prędkości transmisji:
 - i. 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a
 - ii. MCS0-MCS31 (6,5Mbps do 600Mbps) dla 802.11n
 - iii. MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac
 - iv. MCS0-MCS11, NSS= 1-4 (3,6 Mbps do 2402 Mbps dla 5 GHz) dla 802.11ax
- f. Obsługa HT – kanały 20/40MHz dla 802.11n.
- g. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac.
- h. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax.
- i. Wsparcie dla technologii DFS (Dynamic frequency selection).
- j. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac.
- k. Wsparcie dla:
 - i. MRC (Maximal ratio combining)
 - ii. CDD/CSD (Cyclic delay/shift diversity)
 - iii. STBC (Space-time block coding)
 - iv. LDPC (Low-density parity check)
 - v. Technologia TxBF

29. Specyfikacja radia 802.11b/g/n/ax:

- a. Częstotliwość 2,400 ~2,4835.
- b. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA.
- c. Typy modulacji – CCK, BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.
- d. Moc transmisji konfigurowalna przez administratora.
- e. Prędkości transmisji:
 - i. 1,2,5,11 Mbps dla 802.11b
 - ii. 6,9,12,18,24,36,48,54 Mbps dla 802.11g
 - iii. MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n
 - iv. MCS0-MCS11, NSS= 1-4 (3,6 Mbps do 1147 Mbps) dla 802.11ax

30. Punkt dostępowy musi posiadać co najmniej:

- a. 2 interfejsy 2,5Gbps i 5 Gbps zgodne z standardem 802.3bz:
 - i. z funkcją auto-sensing link oraz MDI/MDX
 - ii. z funkcją PoE/PoE+
- b. Wsparcie dla LACP

		<ul style="list-style-type: none">c. 1 interfejs konsolid. zasilanie zgodne z 802.3ate. przycisk przywracający konfigurację fabrycznąf. port USB 2.0g. slot zabezpieczający Kensington <p>31. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac/ax.</p> <p>32. Parametry pracy urządzenia:</p> <ul style="list-style-type: none">a. Temperatura otoczenia (zakres minimalny): 0-50 ° Cb. Wilgotność (zakres minimalny): 5% - 93%
2.	Pozostałe wymagania	<ul style="list-style-type: none">1. Punkty dostępowe muszą być objęte minimum 36-miesięczną gwarancją producenta. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 45 dni przesyła zamiennik.2. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.3. Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych4. Wszystkie urządzenia muszą być fabrycznie nowe.

Access Point, konfiguracja 3, 2 szt.

Lp.	Wymaganie	Opis warunków spełnienia wymagań
3.	Wymagania funkcjonalne	<ol style="list-style-type: none"> 1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. 2. Punkt dostępowy musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz (standard 802.11a/n/ac wave 2/ax) oraz 2.4GHz (standard 802.11b/g/n/ax). 3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: <ol style="list-style-type: none"> a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https. b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki. c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI oraz CLI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 4. Musi być zapewniona funkcja wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: <ol style="list-style-type: none"> a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego. b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny. c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe. d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję. e. Wirtualny kontroler musi posiadać adres IP, za pomocą którego można zarządzać klastrem. Adres ten, w przypadku awarii musi podążać za nowym wirtualnym kontrolerem i pozostawać bez zmian. f. W ramach jednej grupy (klastra) musi być możliwe używanie Punktów Dostępowych różnego typu, np. w standardzie 802.11n i 802.11ac, które są zarządzane za pomocą tego samego wirtualnego kontrolera. g. Zamawiający wymaga, aby w ramach jednego klastra istniała możliwość pracy minimum 120 urządzeń .



5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
6. Punkt dostępowy musi mieć możliwość pracy jako analizator widma.
7. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa.
8. W system musi być wbudowany serwer DHCP.
9. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
10. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
 - a. EAP-TLS
 - b. PEAP-MSCHAPv2
 - c. PEAP-GTC
 - d. TTLS-MSCHAPv2
11. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP.
12. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID.
13. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
14. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
 - a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania.
 - b. Zewnętrzny portal WWW.
15. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
16. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
17. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
 - a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe.
 - b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu.
 - c. Rozkład ruchu pomiędzy różnymi punktami dostępowym oraz pasmami bazując na ilości użytkowników oraz użyciu pasma.

		<ul style="list-style-type: none">d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału.e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz.f. Wsparcie dla 802.11d oraz 802.11h.g. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane. <p>18. Minimalizacja interferencji związanych z sieciami 3G/4G LTE.</p> <p>19. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej.</p> <p>20. Obsługa roamingu klientów w warstwie 2.</p> <p>21. Obsługa monitoringu przez SNMP.</p> <p>22. Obsługa logowania na zewnętrznym serwerze SYSLOG.</p> <p>23. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.</p> <p>24. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.</p> <p>25. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:</p> <ul style="list-style-type: none">a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością.b. Wykorzystanie pasma.c. Ilość klientów korzystających z systemu/interferujących.d. Ilość ramek wejściowych/wyjściowych dla każdego radia.e. Ilość odrzuconych /błędnych ramek/ dla każdego radia.f. Szum tła dla każdego radia.g. Wyświetlanie logów systemowych. <p>26. Punkt dostępowy musi posiadać 4 wbudowane anteny do pracy w trybie 4x4 MIMO o parametrach uzysku 3,5 dBi dla pasma 2,4 Ghz oraz 5,4 dBi dla pasma 5 GHz.</p> <p>27. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2, 802.11ax</p> <p>28. Specyfikacja radia 802.11a/n/ac wave 2/ax:</p> <ul style="list-style-type: none">a. Obsługiwane częstotliwości:<ul style="list-style-type: none">- 5.150 ~ 5.250 GHz (low band)- 5.250 ~ 5.350 GHz (mid band)- 5.470 ~ 5.725 GHz (Europa)- 5.725 ~ 5.850 GHz (high band)b. Obsługa technologii OFDM i OFDMA.
--	--	---



		<ul style="list-style-type: none">c. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.d. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm.e. Prędkości transmisji:<ul style="list-style-type: none">i. 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11aii. MCS0-MCS31 (6,5Mbps do 600Mbps) dla 802.11niii. MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11aciv. MCS0-MCS11, NSS= 1-4 (3,6 Mbps do 2402 Mbps dla 5 GHz) dla 802.11axf. Obsługa HT – kanały 20/40MHz dla 802.11n.g. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac.h. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax.i. Wsparcie dla technologii DFS (Dynamic frequency selection).j. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac.k. Wsparcie dla:<ul style="list-style-type: none">i. MRC (Maximal ratio combining)ii. CDD/CSD (Cyclic delay/shift diversity)iii. STBC (Space-time block coding)iv. LDPC (Low-density parity check)v. Technologia TxBF <p>29. Specyfikacja radia 802.11b/g/n/ax:</p> <ul style="list-style-type: none">a. Częstotliwość 2,400 ~2,4835.b. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA.c. Typy modulacji – CCK, BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM.d. Moc transmisji konfigurowalna przez administratora.e. Prędkości transmisji:<ul style="list-style-type: none">i. 1,2,5.5,11 Mbps dla 802.11bii. 6,9,12,18,24,36,48,54 Mbps dla 802.11giii. MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11niv. MCS0-MCS11, NSS= 1-4 (3,6 Mbps do 1147 Mbps) dla 802.11ax <p>30. Punkt dostępowy musi posiadać co najmniej:</p> <ul style="list-style-type: none">a. 2 interfejsy 2,5Gbps i 5 Gbps zgodne z standardem 802.3bz:<ul style="list-style-type: none">i. z funkcją auto-sensing link oraz MDI/MDXii. z funkcją PoE/PoE+b. Wsparcie dla LACP
--	--	--

		<ul style="list-style-type: none"> c. 1 interfejs konsoli d. zasilanie zgodne z 802.3bt e. przycisk przywracający konfigurację fabryczną f. port USB 2.0 g. slot zabezpieczający Kensington <p>31. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac/ax.</p> <p>32. Parametry pracy urządzenia:</p> <ul style="list-style-type: none"> a. Temperatura otoczenia (zakres minimalny): 0-50 ° C b. Wilgotność (zakres minimalny): 5% - 93%
4.	Pozostałe wymagania	<ol style="list-style-type: none"> 1. Punkty dostępowe muszą być objęte minimum 36-miesięczną gwarancją producenta. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 45 dni przesyła zamiennik. 2. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni. 3. Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych 4. Wszystkie urządzenia muszą być fabrycznie nowe.

Zakres wdrożenia sieci

1. Dostawa sprzętu

Dostawa obejmuje:

- Dostarczenie wszystkich punktów dostępowych (access point – AP) oraz niezbędnych akcesoriów (uchwyty montażowe, dokumentacja producenta, zasilacze PoE, niezbędnych do realizacji zamówienia).
- Weryfikację kompletności i integralności dostawy.

2. Montaż fizyczny

Zakres montażu:

- Instalacja punktów dostępowych w miejscach wskazanych przez Zamawiającego.
- Montaż urządzeń na sufitach lub ścianach, zgodnie z zaleceniami producenta oraz planem pokrycia sieci Wi-Fi.
- Podłączenie urządzeń do infrastruktury LAN (switche PoE), zapewnienie poprawnego zasilania i transmisji danych.
- Etykietowanie kabli i urządzeń zgodnie z ustalonym z Zamawiającym standardem.

3. Konfiguracja sieci Instant AP

Koncepcja sieci:

- Wdrożenie architektury sieciowej Instant – sieć bez dodatkowego fizycznego kontrolera.
- Jeden z punktów dostępowych pełni rolę wiodącego Instant AP (Virtual Controller).
- Pozostałe AP automatycznie dołączają do klastra Instant.

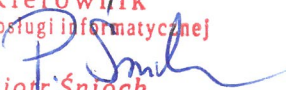
Zakres konfiguracji:

- Utworzenie klastra Instant AP.
- Konfiguracja wirtualnego kontrolera:
 - Parametry sieci (VLAN, IP, DHCP, NAT).
 - Tworzenie i konfiguracja SSID (sieci dla użytkowników, gości, IoT – zgodnie z wymaganiami Zamawiającego).
 - Konfiguracja zabezpieczeń (WPA3, VLAN tagging, segmentacja sieci, Captive Portal).
 - Konfiguracja polityk dostępu, limitów przepustowości, profilowanie urządzeń.
- Konfiguracja roamingu, load balancing i sterowania klientów do pasma 5 GHz.
- Konfiguracja monitorowania pasma i podstawowej ochrony przed nieautoryzowanymi punktami dostępowymi.

4. Uruchomienie systemu i testy

Zakres uruchomienia:

- Uruchomienie klastra Instant.
- Weryfikacja poprawności działania wszystkich punktów dostępowych.
- Testy pokrycia sieci Wi-Fi.
- Testy wydajności i roamingu.
- Weryfikacja poprawnej współpracy wszystkich dostarczonych AP w jednym klastrze.
- Przekazanie Zamawiającemu dokumentacji powykonawczej (schemat sieci, konfiguracja, hasła administracyjne, polityki bezpieczeństwa).
- Szkolenie administratorów w zakresie podstawowego zarządzania i monitorowania klastra Instant AP w wymiarze minimum 3 dni robocze.
- Opracowanie procedury awaryjnej przy awarii wiodącego AP i proces przełączenia na nowy kontroler Instant.

Kierownik
Biura obsługi informatycznej

Piotr Śnióch