Nowy Dwór Mazowiecki, 12. .07.2023 r.

Oznaczenie sprawy: P-041/23

Zapytanie ofertowe z ogłoszeniem

na

„Wymiana urządzeń zapewniających dostęp wifi w Terminalu"

1. **Zamawiający**

   Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o.
   ul. Gen. Wiktora Thommee 1A
   05-102 Nowy Dwór Mazowiecki
   NIP 522-10-25-337
   Tel.: 22 346 40 00
   e-mail: info@modlinairport.pl

2. **Przedmiot zamówienia**

   Przedmiotem zamówienia jest dostawa urządzeń zapewniających dostęp wifi w terminalu, tj. kontrolerów do zarządzania access pointami, plus access pointy na pokrycie zasięgu w Terminalu.

   W ramach realizacji zamówienia Wykonawca zobowiązany będzie, we własnym zakresie, dostarczyć urządzenia stanowiące przedmiot zamówienia, do siedziby Zamawiającego i dokonać jego rozładunku w miejscu wskazanym przez Zamawiającego.

   Szczegółowy Opis przedmiotu zamówienia zawierający minimalne wymagania Zamawiającego w zakresie parametrów technicznych urządzeń, stanowi ***załącznik nr 1*** do zapytania ofertowego.

3. **Postanowienia ogólne**

   3.1 Postępowanie o udzielenie niniejszego zamówienia prowadzone jest w oparciu o postanowienia zawarte w niniejszym dokumencie. Zamawiający jest Zamawiającym sektorowym i z uwagi na wartość zamówienia, która nie przekracza kwoty 431 000 euro, do danego postępowania nie mają zastosowania przepisy ustawy Prawo Zamówień Publicznych.

   3.2 Każdy Wykonawca może złożyć tylko jedną ofertę.

   3.3 Zamawiający nie dopuszcza składania ofert wariantowych.

   3.4 Zamawiający nie przewiduje możliwości udzielenia zamówień uzupełniających.

   3.5 Zamawiający nie przewiduje zwrotu kosztów za przygotowanie oferty również w przypadku unieważnienia postępowania.

4. **Termin realizacji**

   Wykonawca jest zobowiązany zrealizować zamówienie w terminie 4 miesięcy licząc od dnia przekazania zamówienia Wykonawcy. Za dzień przekazania zamówienia Wykonawcy uznaje się dzień jego wysłania na adres e-mail Wykonawcy, wskazany w formularzu ofertowym.

5. **Warunki udziału w postępowaniu**

5.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

1) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2) posiadają wiedzę i doświadczenie do realizacji przedmiotowego zamówienia,
3) dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia,
4) nie podlegają wykluczeniu z postępowania na podstawie przesłanek określonych w oświadczeniu stanowiącym ***załącznik nr 3***.

5.2. Wykonawcy, którzy nie spełnią warunków określonych w pkt 5.1., zostaną wykluczeni z postępowania, a złożone przez nich oferty zostaną odrzucone.

6. **Wymagane oświadczenia i dokumenty**

6.1. W celu potwierdzenia wymagań stawianych przez Zamawiającego, wraz z ofertą Wykonawca składa poniższe oświadczenia i dokumenty:

1) oświadczenie potwierdzające, że Wykonawca spełnia warunki udziału w postępowaniu, zgodnie ze wzorem stanowiącym ***załącznik nr 3*** do niniejszego zapytania;
2) aktualny odpis z Krajowego Rejestru Sądowego albo wydruk z CEIDG, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej — wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

6.2. W uzasadnionych przypadkach Zamawiający może zwrócić się do Wykonawcy o wyjaśnienie złożonej oferty, uzupełnienie niezłożonych dokumentów lub dokumentów zawierających błędy, wyznaczając określony termin na ich uzupełnienie, złożenie wyjaśnień. W tym przypadku dokumenty te powinny być wystawione nie później niż w terminie wskazanym w piśmie wzywającym do uzupełnienia przedmiotowych dokumentów i odzwierciedlać stan prawny na dzień złożenia ofert.

7. **Miejsce oraz termin składania i otwarcia ofert**

7.1. Oferty należy przesyłać za pośrednictwem poczty elektronicznej na adres e-mail: a.blonska@modlinairport.pl lub złożyć bezpośrednio w siedzibie Zmawiającego pod adresem wskazanym w pkt 1, ze wskazaniem tytułu i nr postępowania.

7.2. Termin składania ofert upływa **28. 07. .2023 r. do godz. 12:00**.

7.3. Oferty przesłane lub złożone po terminie nie będą uwzględniane przy ocenie.

8. **Termin związania ofertą**

Wykonawca pozostaje związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

9. **Opis sposobu obliczania ceny oferty**

9.1. Cena oferty jest ceną ryczałtową za świadczenie usługi. W cenie oferty Wykonawca powinien zawrzeć wszelkie koszty wykonania przedmiotu zamówienia, zgodnie z opisem przedmiotu zamówienia. Wynagrodzenie Wykonawcy winno obejmować całość prac stanowiących przedmiot zamówienia oraz zawierać wszelkie koszty poniesione przez Wykonawcę przy wykonywaniu przedmiotowych usług, w tym koszty transportu urządzeń do siedziby Zamawiającego.

9.2. Wymaga się, aby cena oferty została określona jako cena brutto, tj. łącznie z podatkiem VAT.

9.3. Cena powinna być wyrażona w złotych polskich, nie dopuszcza się prowadzenia rozliczeń w walutach obcych.

10. Opis kryteriów i sposobu dokonywania oceny oferty

10.1. Przy wyborze najkorzystniejszej oferty, Zamawiający będzie kierował się kryterium ceny: **cena - 100%.** Za najkorzystniejszą uznana zostanie ważna oferta z najniższą ceną.

10.2. Jeżeli w postępowaniu zostaną złożone dwie oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty do złożenia w wyznaczonym terminie ofert dodatkowych.

10.3. Ceny ofert dodatkowych nie mogą przewyższać cen zaoferowanych pierwotnie.

10.4. W postępowaniu, jako pierwsza sprawdzana będzie oferta z najniższą ceną. Jeśli oferta po ewentualnych wyjaśnieniach okaże się zgodna z treścią zapytania ofertowego dokonywany jest jej wybór. Pozostałe oferty nie podlegają ocenie.

10.5. Niezwłocznie po wyborze oferty najkorzystniejszej, Zamawiający poinformuje Wykonawców, którzy złożyli oferty, o wyborze oferty najkorzystniejszej, podając jej cenę i nazwę Wykonawcy, który ją złożył. Informacja o wyborze opublikowana zostanie również na stronie internetowej Zamawiającego: www.modlinairport.pl

11. Sposób przygotowania oferty

11.1. Koszty związane z przygotowaniem i złożeniem oferty ponosi Wykonawca.

11.2. Oferta powinna zawierać:

1) Wypełniony i podpisany formularz ofertowy, którego wzór został określony w ***załączniku nr 2*** do zapytania.
2) Dokumenty, o których mowa w pkt 6.1. zapytania.

11.3. Wymaga się, aby oferta pod rygorem jej odrzucenia, była podpisana przez osobę lub osoby uprawnione do reprezentowania Wykonawcy. W przypadku, gdy ofertę podpisuje pełnomocnik, do oferty należy załączyć pełnomocnictwo określające zakres umocowania.

12. Oferta wspólna i podwykonawcy

12.1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. Wykonawcy występujący wspólnie muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia lub do reprezentowania ich w postępowaniu i do zawarcia umowy. Uwaga: treść pełnomocnictwa powinna dokładnie określać zakres umocowania.

12.2. W przypadku wspólnego ubiegania się wykonawców o udzielenie zamówienia, wykonawcy muszą spełniać warunki udziału w postępowaniu łącznie.

12.3. W przypadku, gdy Wykonawca przewiduje powierzenie wykonania części prac lub dostaw podwykonawcy, zobowiązany jest w treści oferty wskazać zakres prac lub dostaw wykonywanych przez podwykonawców.

13. Osoby uprawnione do kontaktów z Wykonawcami

Osobą uprawnioną do kontaktów z Wykonawcami jest Anna Błońska – Główny specjalista ds. zamówień i kontraktów, nr tel.: 22 346 41 11, e-mail: a.blonska@modlinairport.pl

14. Informacja o formalnościach, jakie powinny zostać dopełnione po wyborze oferty

14.1. Do Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, Zamawiający prześle zamówienie na realizację przedmiotowego zadania.

14.2. Zamówienie wysłane będzie drogą mailową na wskazany przez Wykonawcę w ofercie adres e-mail.

14.3. Termin realizacji zamówienia liczony jest od momentu przesłania zamówienia przez Zamawiającego na adres e-mail Wykonawcy.

14.4. Wzór zamówienia stanowi ***załącznik nr 4*** do zapytania.

15. Informacja o przetwarzaniu danych

Zgodnie z obowiązkiem wynikającym z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), zwanego dalej RODO, informuję, iż:

1) Administrator danych osobowych

Administratorem Pani/Pana danych osobowych jest Spółka Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o. z siedzibą w ul. Generała Wiktora Thommee 1A, 05-102 Nowy Dwór Mazowiecki, zwaną dalej Spółką.

2) Inspektor Ochrony Danych

Administrator powołał Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w przypadku jakichkolwiek pytań lub uwag dotyczących przetwarzania Pani/Pana danych osobowych i praw przysługujących Pani/Panu na mocy przepisów o ochronie danych osobowych. Dane kontaktowe inspektora ochrony danych: email: inspektor.odo@modlinairport.pl.

3) Cele przetwarzania danych osobowych

A. **Jeśli jest Pani/Pan stroną postępowania** celem przetwarzania danych jest:

a) zawarcie i wykonanie oraz rozliczenie umowy - na podstawie art. 6 ust. 1 lit. b RODO;

b) wypełnienie obowiązków prawnych ciążących na Spółce wynikających m.in. z przepisów skarbowych, o rachunkowości - na podstawie art. 6 ust. 1 lit. c RODO;

c) dochodzenie lub obrona przed roszczeniami co jest prawnie uzasadnionym interesem Spółki - na podstawie art. 6 ust. 1 lit. f RODO;

B. Podanie danych stanowi wymóg zawarcia i realizacji umowy. **Jeśli jest Pani/Pan pracownikiem lub współpracownikiem firmy, która jest stroną postępowania** i została/ł Pani/Pan wskazana/y jako odpowiedzialna/y za realizację poszczególnych zadań wynikających z zamówienia, celem przetwarzania danych jest weryfikacja Pani/Pana kwalifikacji oraz dochodzenie i obrona przed roszczeniami co jest prawnie uzasadnionym interesem Spółki - na podstawie art. 6 ust. 1 lit. f RODO.

Kategorie przetwarzanych Pani/Pana danych osobowych to: imię i nazwisko, pełniona funkcja, adres e-mail, numer telefonu, jeśli to konieczne również kwalifikacje niezbędne do wykonania zamówienia. Dane osobowe zostały pozyskane od Pani/Pana pracodawcy. Podanie danych stanowi wymóg udziału w postępowaniu.

Dane z innych źródeł

Możemy pozyskiwać Pani/Pana dane osobowe z publicznie dostępnych źródeł, takich jak rejestry przedsiębiorców CEIDG lub KRS, rejestr REGON w celu weryfikacji informacji podanych przez uczestnika postępowania. Zakres przetwarzanych danych będzie w takim przypadku ograniczony do danych dostępnych publicznie w odpowiednich rejestrach.

4) **Odbiorcy danych**
Odbiorcami Pani/Pana danych osobowych mogą być firmy świadczące usługi kontroli bezpieczeństwa i kontroli dostępu oraz ochrony osób i mienia na rzecz Spółki Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o., firmy informatyczne wspomagające Administratora, dostawcy usług prawnych i doradczych, firmy kurierskie i pocztowe oraz podmioty, którym Administrator ma obowiązek przekazywania dane na podstawie obowiązujących przepisów prawa np. Straż Graniczna, Policja, Urząd Lotnictwa Cywilnego.

5) **Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej**
Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego ani organizacji międzynarodowej z wyłączeniem sytuacji wynikających z przepisów prawa.

6) **Okres przechowywania danych**
Dane osobowe będą przechowywane przez czas niezbędny do realizacji wyżej wymienionych celów tzn. do czasu zrealizowania umowy, zakończenia okresu gwarancji lub rękojmi, przez czas wymagany przepisami prawa w przypadku danych finansowych, przedawnienia roszczeń lub do czasu wniesienia skutecznego sprzeciwu w zakresie w jakim podstawą przetwarzania jest prawnie uzasadniony interes Spółki.

7) **Uprawnienia osób, których dane dotyczą**
Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych. Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.

8) **Informacje o zautomatyzowanym podejmowaniu decyzji**
Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.

16. Załączniki

1) Opis przedmiotu zamówienia
2) Formularz ofertowy wraz z parametrami technicznymi oferowanego sprzętu
3) Wzór oświadczenia o spełnianiu warunków udziału w postępowaniu
4) Wzór zamówienia

WICEPREZES ZARZĄDU
Grzegorz Hlebowicz

WICEPREZES ZARZĄDU
Tomasz Szymczak

Załącznik nr 1 do zapytania ofertowego

Oznaczenie sprawy: P-041/23

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

A. Bezprzewodowy Punkt Dostępowy – 20 sztuk

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Typ	Wewnętrzny punkt dostępowy bezprzewodowej sieci LAN.
2.	Zastosowanie	Zapewnienie połączenia do sieci komputerowej wykorzystywanej dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
3.	Moduły radiowe WLAN	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). Możliwość przełączenia jednego z modułów radiowych do pracy w paśmie 6GHz, zgodnie z standardem WiFi6E umożliwiające pracę dowolnym trzech trybów: (2,4GHz/5GHz), (2,4GHz/6GHz), (5GHz/6GHz). Wbudowane anteny WiFi typu omnidirectional do pracy trybach 2,4/5/6GHz. Tryby pracy anten i uzysk: • 2x2 MIMO o parametrach uzysku 2,8 dBi dla pasma 2,4 Ghz • 2x2 MIMO o parametrach uzysku 4,5 dBi dla pasma 5 GHz • 2x2 MIMO o parametrach uzysku 4,5 dBi dla pasma 6 GHz
4.	Montaż	Przystosowany do instalacji sufitowej wewnątrz budynków.
5.	Tryb pracy autonomiczny	Praca w trybie autonomicznym, tj. bez nadzoru centralnego kontrolera lub systemu zarządzającego. • Zarządzanie i monitoring przez przeglądarkę internetową i protokół https. • Operacje konfiguracyjne przeprowadzane z poziomu przeglądarki (GUI) lub linii komend (CLI). • Przełączenie punktu dostępowego do pracy z centralnym kontrolerem lub systemem zarządzania wykonywane poprzez zmianę ustawienia trybu pracy urządzenia.
6.	Tryb pracy chmurowy	Możliwość pracy w trybie zależnym od nadrzędnego chmurowego systemu zarządzającego. • Zarządzanie bezpośrednio z systemu zarządzania zainstalowanego w chmurze publicznej.

		• Wszystkie operacje konfiguracyjne i monitoring przeprowadzane z poziomu przeglądarki w systemie zarządzania. Przełączenie punktu dostępowego do pracy z systemem zarządzania wykonywane poprzez zmianę ustawienia trybu pracy urządzenia. Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie systemu zarządzania w przypadku zastosowania takiego trybu pracy.
7.	Tryb pracy z kontrolerem WLAN	Możliwość pracy w trybie dedykowanym kontrolerem sieci WLAN. • Zarządzanie bezpośrednio z kontrolera WLAN • Wszystkie operacje konfiguracyjne i monitoring przeprowadzane z poziomu przeglądarki w kontrolerze WLAN. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem WLAN wykonywane poprzez zmianę trybu pracy urządzenia.
8.	Praca grupowa/ klastrowanie	Wbudowany mechanizm wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: • Automatyczny wybór jednego punktu dostępowego, jako elementu zarządzającego. • W przypadku awarii zarządzającego punktu dostępowego (wirtualnego kontrolera) kolejny punkt dostępowy w sieci przejmuje jego rolę w sposób automatyczny. • Wirtualny kontroler dostępny przez adres IP w celu zarządzania całym klastrem. Adres ten, w przypadku awarii podąża za nowym wirtualnym kontrolerem i pozostaje bez zmian. • Modyfikacja konfiguracji jest propagowana na pozostałe punkty dostępowe. • Obraz systemu operacyjnego jest automatycznie propagowany na pozostałe punkty dostępowe. • W ramach jednej grupy (klastra) możliwe używanie punktów dostępowych różnego typu, np. w standardzie 802.11n i 802.11ac, które są zarządzane za pomocą tego samego wirtualnego kontrolera. • Tworzenie klastra z minimum 128 urządzeniami. • Tworzenie klastra składającego się z punktów dostępowych różnego typu przy wykorzystaniu trybu pracy chmurowej.
9.	Funkcje monitoringu	Wbudowana funkcja umożliwiająca monitorowanie pasma radiowego w celu wykrywania np. fałszywych AP.

		Wbudowana funkcja umożliwiająca analizę widma radiowego na potrzeby diagnostyki środowiska. Wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci (wIDS) Wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci (wIPS).
10.	Firewall	Wbudowana w punkt dostępowy pełnostanowa zapora sieciowa dla warstwy sieci L3-L7
11.	Podstawowe funkcje sieciowe	Wbudowany serwer DHCP. Obsługa monitoringu przez SNMP. Obsługa logowania na zewnętrznym serwerze SYSLOG lub systemie zarządzenia. Terminowanie sesji EAP w nie mniej niż następujących opcjach: • EAP-TLS • PEAP-MSCHAPv2 • PEAP-GTC • TTLS-MSCHAPv2
12.	Sieci bezprzewodowe	Obsługa 16 niezależnych BSSID dla pasma 2,4/5GHz i nie mniej niż 4 BSSID przy pracy w paśmie 6GHz Obsługa do 512 klientów podłączonych do punktu dostępowego Każde SSID z możliwością przypisania w sposób statyczny lub dynamiczny do sieci VLAN. Roaming klientów w warstwie 2.
13.	Uwierzytelnianie	Wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów. Wbudowany serwer uwierzytelniający z obsługą kont gościnnych. Zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT. Możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP. Uwierzytelnianie użytkowników za pomocą portalu WWW poprzez: • Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania, zewnętrzny portal WWW.
14.	Zarządzanie pasmem radiowym	Automatyczne zarządzanie pasmem radiowym punktów dostępowych za pomocą auto-adaptacyjnych mechanizmów takich jak: • Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy

		uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. • Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu. • Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma. • Wykrywanie interferencji oraz miejsc bez pokrycia sygnału. • Automatyczne przekierowywanie/przełączanie klientów, którzy mogą pracować w szybszym pasmie (5GHz lub 6GHz). • Wsparcie dla 802.11h. • Możliwość stworzenia profili czasowych, w których dane SSID ma być rozgłaszane. • Minimalizacja interferencji związanych z sieciami 3G/4G LTE
15.	Interface zarządzania	Interfejs zarządzania (dla trybu autonomicznego i chmurowego) dostarczający następujące informacje o systemie: • Widok diagnostyczny prezentujący problemy z sygnałem/prędkością. • Wykorzystanie pasma. • Ilość klientów korzystających z systemu/interferujących. • Ilość ramek wejściowych/wyjściowych dla każdego radia. • Ilość odrzuconych /błędnych ramek/ dla każdego radia. • Szum tła dla każdego radia. • Wyświetlanie logów systemowych.
16.	Specyfikacja radia 2,4GHz 802.11b/g/n/ax	Częstotliwość 2,400 ~2,4835GHz ISM Moc transmisji konfigurowalna przez administratora. Moc nadawcza +18 dBm Maksymalna prędkość transmisji 287Mb/s
17.	Specyfikacja radia 5GHz 802.11a/n/ac wave 2/ax:	Obsługiwane częstotliwości: • 5.150 ~ 5.250 GHz U-NII-1 • 5.250 ~ 5.350 GHz U-NII-2A • 5.470 ~ 5.725 GHz U-NII-2C • 5.725 ~ 5.850 GHz U-NII-3/ISM • 5. 850 to 5.895 GHz U-NII-4 • 5.925 to 6.425 GHz U-NII-5 Moc transmisji konfigurowalna przez administratora. Moc nadawcza +18 dBm Maksymalna prędkość transmisji 1,2Gb/s

18.	Specyfikacja radia 6GHz 802.11ax	Obsługiwane częstotliwości: • 6.425 to 6.525 GHz U-NII-6 • 6.525 to 6.875 GHz U-NII-7 • 6.875 to 7.125 GHz U-NII-8 Moc transmisji konfigurowalna przez administratora Moc nadawcza +18 dBm Maksymalna prędkość transmisji 2,4Gb/s
19.	Technologie Radiowe	Obsługa technologii Orthogonal frequency-division multiplexing (OFDM) i Orthogonal frequency-division multiple access (OFDMA). Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM. Obsługa HT – kanały 20/40MHz dla 802.11n. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax. Wsparcie dla technologii DFS (Dynamic frequency selection). Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac. Wsparcie dla: • MRC (Maximal ratio combining) • CDD/CSD (Cyclic delay/shift diversity) • STBC (Space-time block coding) • LDPC (Low-density parity check) • Technologia TxBF • 802.11ax Target Wait Time (TWT) • 802.11mc Fine Timing Measurement (FTM)
20.	Specyfikacja radia Bluetooth Low Energy (BLE5.0)	Wbudowany moduł radiowy Bluetooth Low Energy (BLE5.0) BLE: moc nadawcza do 5dBm (clasa 1), czułość odbiornika -100dBm. Zintegrowana antena typu omnidirectional BLE/ZigBee o parametrach uzysku 2,6 dBi Wbudowany moduł odbiornika GPS (GNSS L1 (1575.42MHz)) pracujący z czułością -162dBm dla trybu tracking
21.	Sieć LAN	1 interfejs Ethernet 2,5Gbps zgodny z standardem 802.3bz i NBase-T: • prędkości: 100/1000/2500BASE-T • funkcja auto-sensing link oraz MDI/MDX • funkcja PoE/PoE+ • wsparcie dla 802.3az Energy Efficient Ethernet (EEE)
22.	Elementy dodatkowe	1 interfejs konsoli Przycisk przywracający konfigurację fabryczną. Port USB min 2.0 umożliwiający podłączenie i zasilenie urządzeń USB z mocą do 5W

		Slot zabezpieczający Kensington. Port USB musi umożliwiać zainstalowanie urządzenia typu USB LTE Modem na potrzeby bezpośredniego połączenia urządzenia z siecią Internet. Diody LED sygnalizujące stan pracy urządzenia. Wbudowany moduł TPM (Trusted Platform Module).
23.	Zasilanie	Zasilanie PoE zgodne z 802.3at Zasilanie przez zewnętrzny zasilacz DC Maksymalny pobór mocy 14,7W (bez dołączonego urządzenia USB) Dostępny tryb pracy idle Dostępny tryb pracy deep-sleep
24.	Certyfikaty i standardy	Certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac/ax. CE Marked RED Directive 2014/53/EU (lub nowszy) EMC Directive 2014/30/EU (lub nowszy) Low Voltage Directive 2014/35/EU (lub nowszy) UL/IEC/EN 60950 (lub nowszy) EN 60601-1-1, EN60601-1-2 (lub nowsze) Wi-Fi Alliance (WFA): Wi-Fi CERTIFIED a, b, g, n, ac Wi-Fi CERTIFIED 6E (ax, 6GHz) WPA, WPA2 and WPA3 - Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband Passpoint (release 2) Bluetooth SIG Zigbee Alliance Producent urządzania musi być umieszczony w aktualnym raporcie Magic Quadrant Gartner: Enterprise Wired and Wireless LAN Infrastructure
25.	Parametry środowiskowe	Temperatura otoczenia (zakres minimalny): 0-50 º C Wilgotność (zakres minimalny): 5% - 95% Mean Time Between Failure (MTBF): 540000 godzin
26.	Waga i wymiary	Szerokość – maksymalnie 30 cm Głębokość – maksymalnie 30 cm Wysokość (bez montażu) – maksymalnie 10 cm
27.	Mocowania	Wraz z urządzeniem wymagane jest dostarczenie mocowania do sufitu

28.	Warunki gwarancji	• Minimum 3 lata gwarancji producenta; • Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 60 dni przesyła zamiennik. • Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany. • 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. • Wszystkie urządzenia muszą być fabrycznie nowe. • Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta. • Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji ograniczonych czasowo.

B. Kontrolery sieci bezprzewodowej – zestaw 2 kontrolerów pracujących w klastrze niezawodnościowym

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Architektura	Dwa niezależne, fizyczne kontrolery, pracujące w klastrze HA Active/Standby. Kontrolery sieci WLAN w formie fizycznych appliance'ów możliwe do zamontowania w szafie typu rack i wysokości 1U. Dostarczone rozwiązanie musi zarządzać siecią bezprzewodową złożoną z minimum 20 punktów dostępowych z możliwością rozbudowy za pomocą licencji do obsługi sumarycznie 256 punktów dostępowych. Zamawiający wymaga, aby ruch pomiędzy kontrolerem a punktem dostępowym był tunelowany. Kontrolery muszą w pełni obsługiwać dostarczane bezprzewodowe punkty dostępowe oferowane zgodnie z postępowaniem.

		Wbudowana pełnostanowa zapora sieciowea (stateful firewall). Wbudowana funkcja VPN Gateway. Kontrolery musi mieć możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym. Jeżeli do realizacji tego wymagania konieczne są dodatkowe komponenty czy licencje to nie są one wymagane w chwili obecnej. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania. Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jeden kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom.
2.	Wymagania funkcjonalne	Kontroler musi posiadać następujące parametry sieciowe: • możliwość wdrożenia w warstwie 2 i 3 ISO/OSI; • wsparcie dla sieci VLAN w tym również trunk 802.1q; • wbudowany serwer DHCP; • obsługa SNMPv2, SNMPv3; • routing dynamiczny OSPF. Kontroler sieci WLAN musi obsługiwać co najmniej: Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST , DES, 3DES, AES-CBC. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit. Autoryzację dostępu użytkowników: Typy uwierzytelnienia: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia.

		Wsparcie dla autoryzacji, minimum: Microsoft NPS, CISCO NAC, Juniper NAC, Aruba NAC. Kontroler umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal". Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES). Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym. Musi być dostępna opcja terminowania ruchu z sieci WLAN na punkcie dostępowym. Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACS+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli. Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA. Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal). Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla

		osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni).
3.	Wydajność i tablice	Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi: • Możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 20 z możliwością rozbudowy do 250. • Minimalna liczba obsługiwanych sieci VLAN 4096. • Tablica rouingu OSPF co najmniej 1000 wpisów • Liczba obsługiwanych BSSID nie mniej niż 800. • Liczba aktywnych sesji zapory sieciowej nie mniej niż 1mln. • Liczba jednoczesnych tuneli GRE nie mniej niż 4096. • Liczba jednocześnie obsługiwanych adresów MAC nie mniej niż 8000. • Liczba wpisów ARP nie mniej niż 8000 • Liczba klientów DHCP nie mniej niż 8000 • Przepustowość interfejsu fizycznego co najmniej 10 Gbps.
4.	Zarządzanie pasmem radiowym	Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci: Integracja jednoczesnej transmisji danych i głosu. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p. Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming). Ograniczanie pasma dla użytkownika oraz dla roli użytkownika. Ograniczenie pasma dla poszczególnych aplikacji. Ograniczenie pasma dla poszczególnych SSID. Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym: • Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. • Stałe monitorowanie pasma oraz usług.

		• Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi. • Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma. • Przełączania użytkowników zdolnych pracować w szybszym paśmie do pracy w tymże paśmie. • Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b). • Wykrywanie interferencji oraz miejsc bez pokrycia sygnału. • Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w. • Integracja z systemami bezpieczeństwa firm trzecich poprzez wbudowane API.
5.	Zapora Sieciowa	Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej, co najmniej następujące własności: • Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia. • Kopiowanie (mirroring) sesji. • Szczegółowe logi (per pakiet) do późniejszej analizy. • ALG (Application Layer Gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP. • Translacja źródłowa, docelowa adresów IP. • Identyfikacja i blokowanie ataków DoS. • Obsługa protokołu GRE. • Deep packet inspection (DPI). • Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach, których używają klienci wifi.
6.	WIPS/WIDS	Kontroler musi posiadać funkcję systemu WIDS/ WIPS. Moduł funkcjonalny WIPS musi posiadać co najmniej następujące funkcje: • Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów. • Identyfikacja i możliwość blokowania sieci Adhoc • Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging • Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler • Identyfikacja błędów konfiguracji klientów WLAN

		• Identyfikacja podszywania się pod autoryzowane punkty dostępowe • Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników. • Jeżeli funkcjonalności WIPS/WIDS opisane powyżej wymagają dodatkowych licencji to licencje te są wymagane w chwili uruchomienia systemu.
7.	Warunki gwarancji	• Minimum 3 lenia gwarancja producenta obejmująca oprogramowanie kontrolera. • Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7. • Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany. • Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. • 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. • Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta. • Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji ograniczonych czasowo.

Załącznik nr 2 do zapytania ofertowego

Oznaczenie sprawy: P-041/23

Formularz ofertowy

Składając ofertę w imieniu *(w przypadku podmiotów występujących wspólnie wymienić wszystkich wykonawców składających ofertę)*

Nazwa Wykonawcy .....

z siedzibą .....

Tel. ....., e-mail: .....

NIP....., REGON .....

dla Spółki Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o., w prowadzonym postępowaniu o udzielenie zamówienia w trybie zapytania ofertowego z ogłoszeniem, na ***Wymianę urządzeń zapewniających dostęp wifi w Terminalu,*** oferujemy wykonanie przedmiotu zamówienia w wymaganym terminie, zgodnie z warunkami zapytania ofertowego nr **P-041/23** z dnia ..... .2023 r.,
za cenę ryczałtową w wysokości:

brutto ..... zł

(słownie: .....)

kwota podatku VAT ..... zł

w wysokości netto ..... zł

W cenę wliczyliśmy wszystkie niezbędne koszty związane z realizacją zamówienia, o których mowa w Zapytaniu ofertowym.

1. Przedmiot zamówienia będzie przez nas zrealizowany w terminie do 4 miesięcy licząc od dnia przesłania drogą mailową zamówienia na adres e-mail wskazany w niniejszym formularzu.
2. Oświadczamy, iż zapoznaliśmy się z warunkami uczestnictwa w postępowaniu i nie wnosimy do nich zastrzeżeń oraz otrzymaliśmy wszelkie niezbędne informacje do przygotowania oferty.
3. Akceptujemy czas związania ofertą – 30 dni. Termin ten rozpoczyna się wraz z upływem terminu składania ofert.
4. Płatność zrealizowana będzie przez Zamawiającego przelewem na rachunek bankowy Wykonawcy podany na fakturze, w terminie 30 dni od daty prawidłowego otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT.

5. Akceptujemy treść wzoru zamówienia, stanowiącego ***załącznik nr 4*** do zapytania ofertowego i w razie wybrania naszej oferty zobowiązujemy się do jego realizacji na warunkach w nim opisanych.
6. Informujemy, że niżej wymieniony zakres zamówienia zamierzamy wykonać przy pomocy podwykonawców:

   .....

   (wpisać zakres prac lub „nie dotyczy")

   .....
7. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia w niniejszym postępowaniu.*
8. Ofertę składamy na ..... ponumerowanych stronach w sposób ciągły, wraz z załącznikami które stanowią:
   1) .....
   2) .....
   3) .....
   4) .....
   5) .....

..... , dnia .....

miejscowość *data*

.....

podpis Wykonawcy

Jednocześnie oświadczamy, że ofertowane przez nas urządzenia są zgodne z wymaganiami Zamawiającego opisanymi w treści zapytania ofertowego. Na potwierdzenie niniejszego składamy poniższy wykaz zgodności z parametrami technicznymi.

---

[1] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

* W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

A. Bezprzewodowy Punkt Dostępowy – 20 sztuk

Producent urządzenia .....

Model urządzenia .....

Cena netto za 1 sztukę .....

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Oświadczenie Wykonawcy o zgodności / braku zgodności urządzenia z wymaganiami Zamawiającego */proszę wpisać TAK lub NIE/*
1.	Typ	Wewnętrzny punkt dostępowy bezprzewodowej sieci LAN.	
2.	Zastosowanie	Zapewnienie połączenia do sieci komputerowej wykorzystywanej dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.	
3.	Moduły radiowe WLAN	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). Możliwość przełączenia jednego z modułów radiowych do pracy w paśmie 6GHz, zgodnie z standardem WiFi6E umożliwiające pracę dowolnym trzech trybów: (2,4GHz/5GHz), (2,4GHz/6GHz), (5GHz/6GHz). Wbudowane anteny WiFi typu omnidirectional do pracy trybach 2,4/5/6GHz. Tryby pracy anten i uzysk: • 2x2 MIMO o parametrach uzysku 2,8 dBi dla pasma 2,4 Ghz • 2x2 MIMO o parametrach uzysku 4,5 dBi dla pasma 5 GHz • 2x2 MIMO o parametrach uzysku 4,5 dBi dla pasma 6 GHz	
4.	Montaż	Przystosowany do instalacji sufitowej wewnątrz budynków.	
5.	Tryb pracy autonomiczny	Praca w trybie autonomicznym, tj. bez nadzoru centralnego kontrolera lub systemu zarządzającego. • Zarządzanie i monitoring przez przeglądarkę internetową i protokół https.	

		• Operacje konfiguracyjne przeprowadzane z poziomu przeglądarki (GUI) lub linii komend (CLI). • Przełączenie punktu dostępowego do pracy z centralnym kontrolerem lub systemem zarządzania wykonywane poprzez zmianę ustawienia trybu pracy urządzenia.	
6.	Tryb pracy chmurowy	Możliwość pracy w trybie zależnym od nadrzędnego chmurowego systemu zarządzającego. • Zarządzanie bezpośrednio z systemu zarządzania zainstalowanego w chmurze publicznej. • Wszystkie operacje konfiguracyjne i monitoring przeprowadzane z poziomu przeglądarki w systemie zarządzania. Przełączenie punktu dostępowego do pracy z systemem zarządzania wykonywane poprzez zmianę ustawienia trybu pracy urządzenia. Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie systemu zarządzania w przypadku zastosowania takiego trybu pracy.	
7.	Tryb pracy z kontrolerem WLAN	Możliwość pracy w trybie dedykowanym kontrolerem sieci WLAN. • Zarządzanie bezpośrednio z kontrolera WLAN • Wszystkie operacje konfiguracyjne i monitoring przeprowadzane z poziomu przeglądarki w kontrolerze WLAN. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem WLAN wykonywane poprzez zmianę trybu pracy urządzenia.	
8.	Praca grupowa/ klastrowanie	Wbudowany mechanizm wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: • Automatyczny wybór jednego punktu dostępowego, jako elementu zarządzającego. • W przypadku awarii zarządzającego punktu dostępowego (wirtualnego kontrolera) kolejny punkt dostępowy w sieci przejmuje jego rolę w sposób automatyczny. • Wirtualny kontroler dostępny przez adres IP w celu zarządzania całym klastrem. Adres ten, w przypadku awarii podąża za nowym wirtualnym kontrolerem i pozostaje bez zmian.	

		• Modyfikacja konfiguracji jest propagowana na pozostałe punkty dostępowe. • Obraz systemu operacyjnego jest automatycznie propagowany na pozostałe punkty dostępowe. • W ramach jednej grupy (klastra) możliwe używanie punktów dostępowych różnego typu, np. w standardzie 802.11n i 802.11ac, które są zarządzane za pomocą tego samego wirtualnego kontrolera. • Tworzenie klastra z minimum 128 urządzeniami. • Tworzenie klastra składającego się z punktów dostępowych różnego typu przy wykorzystaniu trybu pracy chmurowej.	
9.	Funkcje monitoringu	Wbudowana funkcja umożliwiająca monitorowanie pasma radiowego w celu wykrywania np. fałszywych AP. Wbudowana funkcja umożliwiająca analizę widma radiowego na potrzeby diagnostyki środowiska. Wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci (wIDS) Wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci (wIPS).	
10.	Firewall	Wbudowana w punkt dostępowy pełnostanowa zapora sieciowa dla warstwy sieci L3-L7	
11.	Podstawowe funkcje sieciowe	Wbudowany serwer DHCP. Obsługa monitoringu przez SNMP. Obsługa logowania na zewnętrznym serwerze SYSLOG lub systemie zarządzenia. Terminowanie sesji EAP w nie mniej niż następujących opcjach: • EAP-TLS • PEAP-MSCHAPv2 • PEAP-GTC • TTLS-MSCHAPv2	
12.	Sieci bezprzewodowe	Obsługa 16 niezależnych BSSID dla pasma 2,4/5GHz i nie mniej niż 4 BSSID przy pracy w paśmie 6GHz Obsługa do 512 klientów podłączonych do punktu dostępowego Każde SSID z możliwością przypisania w sposób statyczny lub dynamiczny do sieci VLAN. Roaming klientów w warstwie 2.	

13.	Uwierzytelnianie	Wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów. Wbudowany serwer uwierzytelniający z obsługą kont gościnnych. Zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT. Możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP. Uwierzytelnianie użytkowników za pomocą portalu WWW poprzez: • Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania, zewnętrzny portal WWW.	
14.	Zarządzanie pasmem radiowym	Automatyczne zarządzanie pasmem radiowym punktów dostępowych za pomocą auto-adaptacyjnych mechanizmów takich jak: • Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. • Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu. • Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma. • Wykrywanie interferencji oraz miejsc bez pokrycia sygnału. • Automatyczne przekierowywanie/przełączanie klientów, którzy mogą pracować w szybszym pasmie (5GHz lub 6GHz). • Wsparcie dla 802.11h. • Możliwość stworzenia profili czasowych, w których dane SSID ma być rozgłaszane. • Minimalizacja interferencji związanych z sieciami 3G/4G LTE	
15.	Interface zarządzania	Interfejs zarządzania (dla trybu autonomicznego i chmurowego) dostarczający następujące informacje o systemie: • Widok diagnostyczny prezentujący problemy z sygnałem/prędkością.	

		• Wykorzystanie pasma. • Ilość klientów korzystających z systemu/interferujących. • Ilość ramek wejściowych/wyjściowych dla każdego radia. • Ilość odrzuconych /błędnych ramek/ dla każdego radia. • Szum tła dla każdego radia. • Wyświetlanie logów systemowych.	
16.	Specyfikacja radia 2,4GHz 802.11b/g/n/ax	Częstotliwość 2,400 ~2,4835GHz ISM Moc transmisji konfigurowalna przez administratora. Moc nadawcza +18 dBm Maksymalna prędkość transmisji 287Mb/s	
17.	Specyfikacja radia 5GHz 802.11a/n/ac wave 2/ax:	Obsługiwane częstotliwości: • 5.150 ~ 5.250 GHz U-NII-1 • 5.250 ~ 5.350 GHz U-NII-2A • 5.470 ~ 5.725 GHz U-NII-2C • 5.725 ~ 5.850 GHz U-NII-3/ISM • 5. 850 to 5.895 GHz U-NII-4 • 5.925 to 6.425 GHz U-NII-5 Moc transmisji konfigurowalna przez administratora. Moc nadawcza +18 dBm Maksymalna prędkość transmisji 1,2Gb/s	
18.	Specyfikacja radia 6GHz 802.11ax	Obsługiwane częstotliwości: • 6.425 to 6.525 GHz U-NII-6 • 6.525 to 6.875 GHz U-NII-7 • 6.875 to 7.125 GHz U-NII-8 Moc transmisji konfigurowalna przez administratora Moc nadawcza +18 dBm Maksymalna prędkość transmisji 2,4Gb/s	
19.	Technologie Radiowe	Obsługa technologii Orthogonal frequency-division multiplexing (OFDM) i Orthogonal frequency-division multiple access (OFDMA). Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM. Obsługa HT – kanały 20/40MHz dla 802.11n. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax. Wsparcie dla technologii DFS (Dynamic frequency selection).	

		Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac. Wsparcie dla: • MRC (Maximal ratio combining) • CDD/CSD (Cyclic delay/shift diversity) • STBC (Space-time block coding) • LDPC (Low-density parity check) • Technologia TxBF • 802.11ax Target Wait Time (TWT) • 802.11mc Fine Timing Measurement (FTM)	
20.	Specyfikacja radia Bluetooth Low Energy (BLE5.0)	Wbudowany moduł radiowy Bluetooth Low Energy (BLE5.0) BLE: moc nadawcza do 5dBm (clasa 1), czułość odbiornika -100dBm. Zintegrowana antena typu omnidirectional BLE/ZigBee o parametrach uzysku 2,6 dBi Wbudowany moduł odbiornika GPS (GNSS L1 (1575.42MHz)) pracujący z czułością -162dBm dla trybu tracking	
21.	Sieć LAN	1 interfejs Ethernet 2,5Gbps zgodny z standardem 802.3bz i NBase-T: • prędkości: 100/1000/2500BASE-T • funkcja auto-sensing link oraz MDI/MDX • funkcja PoE/PoE+ • wsparcie dla 802.3az Energy Efficient Ethernet (EEE)	
22.	Elementy dodatkowe	1 interfejs konsoli Przycisk przywracający konfigurację fabryczną. Port USB min 2.0 umożliwiający podłączenie i zasilenie urządzeń USB z mocą do 5W Slot zabezpieczający Kensington. Port USB musi umożliwiać zainstalowanie urządzenia typu USB LTE Modem na potrzeby bezpośredniego połączenia urządzenia z siecią Internet. Diody LED sygnalizujące stan pracy urządzenia. Wbudowany moduł TPM (Trusted Platform Module).	
23.	Zasilanie	Zasilanie PoE zgodne z 802.3at Zasilanie przez zewnętrzny zasilacz DC Maksymalny pobór mocy 14,7W (bez dołączonego urządzenia USB) Dostępny tryb pracy idle Dostępny tryb pracy deep-sleep	

24.	Certyfikaty i standardy	Certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac/ax. CE Marked RED Directive 2014/53/EU (lub nowszy) EMC Directive 2014/30/EU (lub nowszy) Low Voltage Directive 2014/35/EU (lub nowszy) UL/IEC/EN 60950 (lub nowszy) EN 60601-1-1, EN60601-1-2 (lub nowsze) Wi-Fi Alliance (WFA): Wi-Fi CERTIFIED a, b, g, n, ac Wi-Fi CERTIFIED 6E (ax, 6GHz) WPA, WPA2 and WPA3 - Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband Passpoint (release 2) Bluetooth SIG Zigbee Alliance Producent urządzania musi być umieszczony w aktualnym raporcie Magic Quadrant Gartner: Enterprise Wired and Wireless LAN Infrastructure	
25.	Parametry środowiskowe	Temperatura otoczenia (zakres minimalny): 0-50 º C Wilgotność (zakres minimalny): 5% - 95% Mean Time Between Failure (MTBF): 540000 godzin	
26.	Waga i wymiary	Szerokość – maksymalnie 30 cm Głębokość – maksymalnie 30 cm Wysokość (bez montażu) – maksymalnie 10 cm	
27.	Mocowania	Wraz z urządzeniem wymagane jest dostarczenie mocowania do sufitu	
28.	Warunki gwarancji	• Minimum 3 lata gwarancji producenta; • Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 60 dni przesyła zamiennik. • Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany. • Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. • Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego	Wymiar gwarancji: ..... lata Pozostałe wymagania: ..... */wpisać TAK lub NIE/*

		przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych. • Wszystkie urządzenia muszą być fabrycznie nowe. • Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta. • Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji ograniczonych czasowo.	

B. Kontrolery sieci bezprzewodowej – zestaw 2 kontrolerów pracujących w klastrze niezawodnościowym

Producent urządzenia .....

Model urządzenia .....

Cena netto za 1 sztukę .....

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Oświadczenie Wykonawcy o zgodności / braku zgodności urządzenia z wymaganiami Zamawiającego */proszę wpisać TAK lub NIE/*
1.	Architektura	Dwa niezależne, fizyczne kontrolery, pracujące w klastrze HA Active/Standby. Kontrolery sieci WLAN w formie fizycznych appliance'ów możliwe do zamontowania w szafie typu rack i wysokości 1U. Dostarczone rozwiązanie musi zarządzać siecią bezprzewodową złożoną z minimum 20 punktów dostępowych z możliwością rozbudowy za pomocą licencji do obsługi sumarycznie 256 punktów dostępowych. Zamawiający wymaga, aby ruch pomiędzy kontrolerem a punktem dostępowym był tunelowany.	

		Kontrolery muszą w pełni obsługiwać dostarczane bezprzewodowe punkty dostępowe oferowane zgodnie z postępowaniem. Wbudowana pełnostanowa zapora sieciowea (stateful firewall). Wbudowana funkcja VPN Gateway. Kontrolery musi mieć możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym. Jeżeli do realizacji tego wymagania konieczne są dodatkowe komponenty czy licencje to nie są one wymagane w chwili obecnej. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania. Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jeden kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom.	
2.	Wymagania funkcjonalne	Kontroler musi posiadać następujące parametry sieciowe: • możliwość wdrożenia w warstwie 2 i 3 ISO/OSI; • wsparcie dla sieci VLAN w tym również trunk 802.1q; • wbudowany serwer DHCP; • obsługa SNMPv2, SNMPv3; • routing dynamiczny OSPF. Kontroler sieci WLAN musi obsługiwać co najmniej: Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST , DES, 3DES, AES-CBC. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit. Autoryzację dostępu użytkowników: Typy uwierzytelnienia: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC	

		2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia. Wsparcie dla autoryzacji, minimum: Microsoft NPS, CISCO NAC, Juniper NAC, Aruba NAC. Kontroler umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal". Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES). Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym. Musi być dostępna opcja terminowania ruchu z sieci WLAN na punkcie dostępowym. Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACS+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia.	

		Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli. Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA. Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal). Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni).	
3.	Wydajność i tablice	Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi: • Możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 20 z możliwością rozbudowy do 250. • Minimalna liczba obsługiwanych sieci VLAN 4096. • Tablica rouingu OSPF co najmniej 1000 wpisów • Liczba obsługiwanych BSSID nie mniej niż 800. • Liczba aktywnych sesji zapory sieciowej nie mniej niż 1mln. • Liczba jednoczesnych tuneli GRE nie mniej niż 4096. • Liczba jednocześnie obsługiwanych adresów MAC nie mniej niż 8000. • Liczba wpisów ARP nie mniej niż 8000 • Liczba klientów DHCP nie mniej niż 8000 • Przepustowość interfejsu fizycznego co najmniej 10 Gbps.	
4.	Zarządzanie pasmem radiowym	Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci: Integracja jednoczesnej transmisji danych i głosu. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p. Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming). Ograniczanie pasma dla użytkownika oraz dla roli użytkownika.	

		Ograniczenie pasma dla poszczególnych aplikacji. Ograniczenie pasma dla poszczególnych SSID. Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym: • Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. • Stałe monitorowanie pasma oraz usług. • Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi. • Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma. • Przełączania użytkowników zdolnych pracować w szybszym paśmie do pracy w tymże paśmie. • Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b). • Wykrywanie interferencji oraz miejsc bez pokrycia sygnału. • Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w. • Integracja z systemami bezpieczeństwa firm trzecich poprzez wbudowane API.	
5.	Zapora Sieciowa	Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej, co najmniej następujące własności: • Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia. • Kopiowanie (mirroring) sesji. • Szczegółowe logi (per pakiet) do późniejszej analizy. • ALG (Application Layer Gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP. • Translacja źródłowa, docelowa adresów IP. • Identyfikacja i blokowanie ataków DoS. • Obsługa protokołu GRE. • Deep packet inspection (DPI).	

		• Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach, których używają klienci wifi.	
6.	WIPS/WIDS	Kontroler musi posiadać funkcję systemu WIDS/ WIPS. Moduł funkcjonalny WIPS musi posiadać co najmniej następujące funkcje: • Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów. • Identyfikacja i możliwość blokowania sieci Adhoc • Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging • Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler • Identyfikacja błędów konfiguracji klientów WLAN • Identyfikacja podszywania się pod autoryzowane punkty dostępowe • Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników. • Jeżeli funkcjonalności WIPS/WIDS opisane powyżej wymagają dodatkowych licencji to licencje te są wymagane w chwili uruchomienia systemu.	
7.	Warunki gwarancji	• Minimum 3 lenia gwarancja producenta obejmująca oprogramowanie kontrolera. • Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7. • Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub podmiot przez niego autoryzowany. • Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. • Wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Polski. • Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego	Wymiar gwarancji: ..... lata Pozostałe wymagania: ..... */wpisać TAK lub NIE/*

		przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych. • Wszystkie elementy rozwiązania muszą pochodzić od jednego producenta. • Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne, nie dopuszcza się licencji ograniczonych czasowo.	

.....

podpis Wykonawcy

Załącznik nr 3 do zapytania ofertowego

Oznaczenie sprawy: P-041/23

Nazwa Wykonawcy .....

.....

Oświadczenie

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego na ***Wymianę urządzeń zapewniających dostęp wifi w Terminalu,*** oświadczam iż Wykonawca:

1. posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień,
2. posiada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zamówienia,
3. znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
4. nie podlega wykluczeniu z postępowania na podstawie przesłanek zawartych poniżej,

- w zakresie wymaganym przez Zamawiającego.

Jednocześnie oświadczamy/y, iż nie podlegam/y wykluczeniu z postępowania o udzielenie zamówienia na podstawie poniżej określonych przesłanek.

Zamawiający wykluczy z postępowania:

1) wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;
2) wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   a) o którym mowa w art. 165a, art. 181–188, art. 189a, art. 218–221, art. 228–230a, art. 250a, art. 258 lub art. 270–309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2017 r. poz. 1463 i 1600),
   b) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny,
   c) skarbowe,
   d) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769);
3) wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2;

4) wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
5) wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i niedyskryminacyjne kryteria, zwane dalej „kryteriami selekcji", lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;
6) wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;
7) wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
8) wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;
9) wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
10) wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2016 r. poz. 1541 oraz z 2017 r. poz. 734 i 933);
11) wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;
12) wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2017 r. poz. 229, 1089 i 1132), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

.....

podpis Wykonawcy

Załącznik nr 4 do zapytania ofertowego

Oznaczenie sprawy: P-041/23

WZÓR ZAMÓWIENIA

ZAMÓWIENIE NR ...../23

Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o. zwraca się z prośbą o realizację zamówienia na *zakup wraz z dostawą 20 szt. bezprzewodowych punktów dostępowych sieci LAN oraz 2 szt. kontrolerów sieci bezprzewodowej, będących przedmiotem postępowania na* ***„Wymianę urządzeń zapewniających dostęp wifi w Terminalu"***, zgodnie z Państwa ofertą z dnia ..... .2023 r., stanowiącą ***załącznik nr 1*** do zamówienia.

I. **Całkowita wartość zakupu: netto ..... zł** (słownie złotych: .....), powiększona o należny podatek VAT. W cenę zamówienia zostały wliczone wszystkie koszty związane z realizacją zamówienia, w tym:
   1) Cena netto za 1 szt. bezprzewodowego punktu dostępowego (producent, model: .....): ..... zł
   2) Cena netto za 1 szt. kontrolera sieci bezprzewodowej (producent, model: .....): ..... zł

II. **Termin realizacji zamówienia: do 4 miesięcy** od daty złożenia zamówienia. Przez złożenie zamówienia rozumie się przesłanie niniejszego zamówienia drogą mailową na adres elektroniczny Wykonawcy, określony powyżej.
   Za szkody powstałe w związku z realizacją zamówienia, Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania od Wykonawcy na zasadach ogólnych wynikających z Kodeksu cywilnego.

III. **Warunki płatności:**
   1) Płatność nastąpi jednorazowo, przelewem na rachunek bankowy Wykonawcy, wskazany w prawidłowo wystawionej przez Wykonawcę fakturze VAT, w terminie 30 dni od daty jej prawidłowego doręczenia Zamawiającemu.
   2) Podstawą wystawienia faktury będzie podpisany, bez żadnych zastrzeżeń, protokół odbioru przedmiotu zamówienia.
   3) Zamawiający dopuszcza możliwość wystawiania i dostarczania w formie elektronicznej, w formacie PDF: faktur, faktur korygujących oraz duplikatów faktur, zgodnie z art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174 ze zm.).
   4) Dokumenty, o których mowa w pkt 3 powyżej, należy kierować na adres e-mail: faktury.bf@modlinairport.pl
   5) Zamawiający oświadcza, iż posiada status dużego przedsiębiorcy w rozumieniu Ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (Dz. U. 2013 poz. 403 ze zm.).

IV. **Faktura powinna być wystawiona na adres:**
   Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o.
   ul. Generała Wiktora Thommee 1a
   05-102 Nowy Dwór Mazowiecki

NIP: 522-10-25-337

V. **Osoby, po stronie Zamawiającego, upoważnione do odbioru przedmiotu zamówienia oraz kontaktów z Wykonawcą w ramach jego realizacji:**

p. ....., tel. +48 .....; e-mail: .....@modlinairport.pl

VI. **Informacja dot. RODO:**

Klauzula informacyjna Spółki Mazowiecki Port Lotniczy Warszawa-Modlin Sp. z o.o. dotycząca przetwarzania danych osobowych na potrzeby zawierania i realizacji umów handlowych, znajduje się na stronie internetowej www.modlinairport.pl w zakładce „Ochrona Danych Osobowych/Klauzule informacyjne".