

## WZÓR

### UMOWA nr .....

zawarta w Olsztynie, w dniu \_\_\_\_\_ pomiędzy:

**Gminą Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna**, Pl. Jana Pawła II 1, 10-101 Olsztyn, NIP 739-384-70-26, reprezentowaną przez Pana Piotra Grzymowicza - Prezydenta Olsztyna,

w imieniu którego działa Rafał Ruchlewicz – Dyrektor Centrum Informatycznych Usług Wspólnych Olsztyna zwaną dalej „Zamawiającym”

a

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

zwaną/ym dalej „Wykonawcą”,

w wyniku przeprowadzenia przez Zamawiającego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, zgodnie z ustawą Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (t.j. Dz. U. z 2018 r., poz. 1986 z późn. zm.; dalej jako „ustawa pzp”), pn. „zakup systemu WiFi” zawarta została umowa o następującej treści:

#### § 1. PRZEDMIOT UMOWY.

- 1.1. Wykonawca zobowiązany jest dostarczyć Zamawiającemu system WIFI dla obsługi urządzeń, korzystających z sieci bezprzewodowej w jednostkach organizacyjnych Gminy Olsztyn, na który składa się sprzęt wraz z zainstalowanym oprogramowaniem sprzętowym dedykowanym do obsługi WIFI (dalej jako: „System”).
- 1.2. System posiadać będzie:
  - 1) punkty dostępowe (Access Point) – 50 sztuk,
  - 2) aplikację do zarządzania i monitoringu,
  - 3) kontroler,
  - 4) dodatkową funkcjonalność<sup>1</sup> obejmującą egzekwowanie reguł zapory sieciowej w oparciu o użytkowników oraz nadawania priorytetu poszczególnym aplikacjom. Reguły dostępu muszą być centralnie definiowane i egzekwowane dla użytkowników bazując na zdefiniowanej dla nich roli oraz poziomie autoryzacji.
- 1.3. Z zastrzeżeniem ust. 2.1, w terminie uzgodnionym z Zamawiającym Wykonawca zobowiązany jest uruchomić i skonfigurować kontroler z pięcioma punktami dostępowymi (Access Point) we wskazanych przez Zamawiającego lokalizacjach w Olsztynie, przy wykorzystaniu infrastruktury w nich dostępnej (bez montażu dodatkowego okablowania).
- 1.4. System musi być zgodny z parametrami technicznymi i użytkowymi określonymi w Szczegółowym opisie przedmiotu zamówienia stanowiącym załącznik nr 1 do niniejszej umowy (dalej: „SOPZ”) oraz ofertą Wykonawcy stanowiącą załącznik nr 2. Wszystkie urządzenia muszą być dostarczone z wszelkimi elementami wymienionymi w SOPZ.
- 1.5. Wykonawca zapewnia, że System będzie nowy, nieużywany, pochodzący z legalnego kanału dystrybucyjnego producenta Systemu, dopuszczony do dystrybucji i używania w Polsce oraz objęty

<sup>1</sup> Jeżeli została zaoferowana; w przeciwnym wypadku zapis pkt 4) do wykreślenia

gwarancją. Zamawiający jest uprawniony do weryfikacji legalności Systemu i wykorzystywanego w Systemie oprogramowania.

- 1.6. Wykonawca zapewnia, że System jest odpowiedniej jakości i funkcjonalności, a także wolny od wad fizycznych oraz prawnych i nie jest przedmiotem praw lub roszczeń osób trzecich.

## **§ 2.ZASADY REALIZACJI UMOWY.**

- 2.1. Dostarczenie Systemu oraz uruchomienie i skonfigurowanie kontrolera z pięcioma punktami dostępowymi (Access Point), nastąpi w terminie 6 tygodni od daty zawarcia umowy, na koszt i ryzyko Wykonawcy, na adresy w Olsztynie - wskazane przez Zamawiającego. Wraz z Systemem Wykonawca dostarczy Zamawiającemu dokumenty potwierdzające fakt uzyskania przez Zamawiającego uprawnień gwarancyjnych producenta, o których mowa w § 5 Umowy.
- 2.2. Po dostarczeniu Sytemu Zamawiający dokona weryfikacji jego zgodności z wymaganiami określonymi w umowie oraz sprawdzenia pod kątem występowania wad.
- 2.3. W przypadku zgodności Systemu z wymaganiami określonymi w umowie i braku wad oraz prawidłowym działaniu kontrolera z 5 przykładowymi punktami dostępowymi (Access Point), o czym mowa w ust. 1.3, Zamawiający dokona odbioru i podpisze protokół odbioru, którego wzór stanowi załącznik nr 3.
- 2.4. Zamawiający ma prawo zgłoszenia uwag co do zgodności Systemu z umową w razie stwierdzenia jego wady lub nieprawidłowości. W takim przypadku Zamawiający podpisze protokół odbioru z uwagami.
- 2.5. W wypadku zgłoszenia uwag przez Zamawiającego, Wykonawca dostarczy Zamawiającemu System bez wad, zgodnie z wymaganiami określonymi w umowie lub usunie wady bądź nieprawidłowości w inny uzgodniony z Zamawiającym sposób, w terminie 5 dni roboczych. Za dzień roboczy uznaje się dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Polsce zgodnie z ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jedn.: Dz.U. z 2015 r., poz. 90).
- 2.6. Za datę wykonania przedmiotu umowy, o którym mowa w § 1, uważa się datę wskazaną w protokole odbioru przedmiotu umowy bez uwag, o którym mowa w ust. 2.3, wskazującą na termin wykonania przedmiotu umowy określonego w § 1.
- 2.7. Wykonawca zobowiązuje się udzielać Zamawiającemu wszelkich informacji oraz udostępniać wszelkie dokumenty niezbędne do realizacji umowy, w których jest w posiadaniu lub powstałych w związku z jej realizacją.
- 2.8. Wykonawca zobowiązany jest informować niezwłocznie Zamawiającego o wszelkich okolicznościach mogących mieć wpływ na niewykonanie przez niego obowiązków lub mogących mieć wpływ na niedotrzymanie przez niego terminów określonych w umowie, co nie zwalnia go z odpowiedzialności za terminowe i należyte wykonanie umowy. Informacje, o których mowa w zdaniu poprzednim, będą przekazywane Zamawiającemu w formie dokumentowej.

## **§ 3.PRAWO DO KORZYSTANIA.**

- 3.1. Jeżeli korzystanie z elementów Systemu wymaga uzyskania prawa do korzystania z jakiegokolwiek oprogramowania, w szczególności oprogramowanie sterujące kontrolerem i AccessPoint'em, oprogramowanie systemowe, narzędziowe i zarządzające maszyną wirtualną (zwanego dalej „Oprogramowaniem”), Wykonawca zobowiązany jest zapewnić takie prawo do korzystania.
- 3.2. Zapewnienie prawa do korzystania, o którym mowa w ust.3.1, może odbyć się poprzez udzielenie Zamawiającemu licencji lub zapewnienie udzielenia Zamawiającemu licencji przez podmiot uprawniony, bądź przeniesie na Zamawiającego licencji na korzystanie z Oprogramowania albo na podstawie innej formy prawnej korzystania z Oprogramowania, w szczególności w oparciu o tzw. prawa legalnego nabywcy egzemplarza oprogramowania, jednak z wyłączeniem zapewnienia korzystania z Oprogramowania w oparciu o model „Software as a Service”, o ile rozwiązanie to

pozwoli na uzyskanie przez Zamawiającego uprawnień do Oprogramowania, opisanych niniejszą umową.

- 3.3. Zgodnie z przyjętym modelem dystrybucji Oprogramowania, na warunkach wskazanych w ofercie i niniejszej umowie Wykonawca zapewni Zamawiającemu prawo do korzystania z Oprogramowania poprzez .....<sup>2</sup>.
- 3.4. Prawa do korzystania z Oprogramowania nie mogą być wcześniej wykorzystane w innych urządzeniach, muszą pochodzić z legalnego kanału dystrybucyjnego producenta Oprogramowania. W przypadku konieczności aktywacji uprawnień do korzystania, Wykonawca zapewni taką aktywację najpóźniej z momentem instalacji Oprogramowania, np. za pośrednictwem zdalnego dostępu.
- 3.5. Zamawiający zastrzega sobie możliwość kontroli legalności i zgodności z wymaganiami umowy dostarczonego Oprogramowania u jego producenta.
- 3.6. Zamawiający ma prawo korzystać z Oprogramowania na potrzeby prowadzonej przez Zamawiającego działalności, w przypadku licencji lub sublicencji na polach eksploatacji obejmujących trwałe lub czasowe zwielokrotnianie oprogramowania w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, na ilości urządzeń wynikających z przyjętego rozwiązania technicznego budowy Systemu, a niezbędnych do prawidłowego działania Systemu, przez czas nieokreślony.
- 3.7. W przypadku udzielenia licencji lub sublicencji Wykonawca zobowiązuje się, że podmiot uprawniony nie wypowie Zamawiającemu udzielonej licencji z innego powodu niż naruszenie przez Zamawiającego warunków licencyjnych przez okres co najmniej 30 lat. Wypowiedzenie warunków korzystania z Oprogramowania z powodu naruszenia warunków tego korzystania winno być poprzedzone pisemnym wezwaniem do zaniechania naruszeń warunków korzystania i bezskutecznym upływem wyznaczonego Zamawiającemu 30 dniowego terminu na zaniechanie naruszeń.
- 3.8. W przypadku aktualizacji lub poprawek Oprogramowania z dniem udostępnienia aktualizacji lub poprawek Zamawiającemu Wykonawca zapewni udzielenie Zamawiającemu prawa do korzystania z aktualizacji Oprogramowania na zasadach określonych w ust. 3.6.

#### **§ 4.CENA.**

- 4.1. Za realizację przedmiotu umowy, o którym mowa w § 1 , Zamawiający zobowiązuje się zapłacić Wykonawcy cenę w łącznej wysokości \_\_\_\_\_ złotych netto (słownie: \_\_\_\_\_/100), powiększoną o wartość podatku VAT w wysokości: \_\_\_\_\_ zł (słownie: \_\_\_\_\_/100), co daje kwotę brutto: \_\_\_\_\_ zł (słownie: \_\_\_\_\_/100).
- 4.2. Jeżeli Wykonawca posiada firmowy rachunek bankowy związany z prowadzoną działalnością gospodarczą, płatność ceny zostanie dokonana z wykorzystaniem metody podzielonej płatności (split payment). Wykonawca oświadcza, że na wystawionej fakturze zostanie wskazany jego rachunek bankowy związany / niezwiązany<sup>3</sup> z prowadzoną działalnością gospodarczą.
- 4.3. Zapłata ceny nastąpi w formie przelewu na rachunek bankowy Wykonawcy wskazany na fakturze. Zapłata nastąpi w terminie 30 (trzydziestu) dni od dnia wystawienia faktury pod warunkiem doręczenia faktury w terminie 7 (siedmiu) dni od dnia jej wystawienia. W przypadku doręczenia faktury po terminie 7 (siedmiu) dni od dnia jej wystawienia, termin zapłaty ulega wydłużeniu o ilość dni przekroczenia wskazanego wyżej 7 (siedmio) dniowego terminu.
- 4.4. Wykonawca oświadcza, że jest czynnym podatnikiem podatku VAT i zgodnie z art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2018 r., poz. 2174 z późn. zm.) znajduje się w wykazie podmiotów zarejestrowanych jako podatnicy VAT (tzw. biała lista podatników VAT), w którym m.in. ujawniony został numer rachunku bankowego związany z prowadzoną przez

<sup>2</sup> Do opisanego przed zawarciem umowy modelu dystrybucji Oprogramowania na podstawie oferty – przy wykorzystaniu mechanizmów wskazanych w ust. powyżej.

<sup>3</sup> Niepotrzebne skreślić.

Wykonawcę działalnością gospodarczą, służący do rozliczenia transakcji w ramach tej działalności i który zostanie wskazany na fakturze VAT wystawionej Zamawiającemu zgodnie z postanowieniami niniejszego paragrafu. Wykonawca oświadcza, że teraz i na przyszłość zrzeka się wszelkich roszczeń wobec Zamawiającego, w szczególności z tytułu braku terminowej zapłaty wynagrodzenia i wstrzymania się przez Zamawiającego z zapłatą wynagrodzenia w ramach niniejszej umowy w przypadku, gdy okaże się, że wskazany przez Wykonawcę na fakturze VAT numer rachunku bankowego nie będzie w dniu dokonania zapłaty przez Zamawiającego kwoty tytułem wynagrodzenia w ramach niniejszej umowy tożsamy z numerem rachunku bankowego ujawnionym na tzw. białej liście podatników VAT albo nie będzie ujawniony na tzw. białej liście podatników VAT – jeżeli zapłata wynagrodzenia na rachunek Wykonawcy nie ujęty na tzw. białej liście podatników VAT łączyłoby się dla Zamawiającego z jakimikolwiek negatywnymi konsekwencjami prawnymi - do czasu wskazania przez Wykonawcę rachunku bankowego ujawnionego na tzw. białej liście podatników VAT lub ujęcia na tej liście wskazanego wcześniej rachunku bankowego Wykonawcy.

4.5. Faktura będzie wystawiona na:

|                      |  |
|----------------------|--|
| NABYWCA:             | ODBIORCA:  |
| Gmina Olsztyn,       | Centrum Informatycznych Usług Wspólnych Olsztyna |
| Plac Jana Pawła II 1 | Plac Jana Pawła II 1                             |
| 10-101 Olsztyn       | 10-101 Olsztyn                                   |
| NIP: 739-38-47-026   |  |

4.6. Faktura powinna być dostarczona Zamawiającemu w następujący sposób:

- 1) na adres Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1, 10-101 Olsztyn, lub
- 2) na adres e-mail: sekretariat@ciuwo.olsztyn.eu według oświadczenia złożonego przez Strony zgodne z załącznikiem nr 4, lub
- 3) przy użyciu Platformy Elektronicznego Fakturowania (PEF).

4.7. W przypadku, gdy Wykonawca skorzysta z możliwości wysyłania Zamawiającemu faktury (tzw. ustrukturyzowanej faktury elektronicznej) przy użyciu Platformy Elektronicznego Fakturowania, o czym mowa w pkt 4.6.3), numer PEPPOL Zamawiającego to 7393921082. Oprócz danych zawartych w ust. 4.5 w opisie ustrukturyzowanej faktury elektronicznej Wykonawca zobowiązany jest do wskazania numeru i daty zawarcia niniejszej umowy.

4.8. Korekty faktur i noty księgowe (tzw. inne ustrukturyzowane dokumenty elektroniczne) mogą być wysyłane przy użyciu Platformy Elektronicznego Fakturowania, z uwzględnieniem postanowień ust. 4.7.

4.9. Za dzień zapłaty ceny Strony uznają datę obciążenia rachunku bankowego Zamawiającego.

4.10. W przypadku nieterminowej zapłaty należności wynikającej z umowy Zamawiający zapłaci Wykonawcy odsetki w ustawowej wysokości z tytułu opóźnienia.

4.11. Cena obejmuje wszelkie koszty i opłaty związane z realizacją umowy z uwzględnieniem kosztów dostarczenia Systemu, udzielenia gwarancji, a także należnego podatku VAT.

4.12. Podstawą do wystawienia faktury jest podpisany przez Zamawiającego protokół odbioru bez uwag, o którym mowa w ust. 2.3 umowy.

## **§ 5. RĘKOJMIA I GWARANCJA**

5.1. Dostarczony System, określony w ust. 1.1 umowy musi być fabrycznie nowy i objęty .....<sup>4</sup> miesięczną gwarancją producenta na warunkach nie gorszych niż określone w § 5 oraz w pkt 1 ppkt 34, pkt 2

---

<sup>4</sup> Do uzupełnienia przed zawarciem umowy, zgodnie z ofertą wybranego Wykonawcy, nie mniej niż 36 miesięcy.

ppkt 24 i w pkt 3 ppkt. 22 załącznika nr 1 do niniejszej umowy (SOPZ) oraz ofercie Wykonawcy będącej załącznikiem nr 2.

- 5.2. Okres rękojmi na przedmiot zamówienia opisany w § 1 i w SOPZ, stanowiący załącznik nr 1, czasy gotowości serwisowej i czasy naprawy są takie same jak okres, czasy gotowości serwisowej i czasy naprawy w ramach gwarancji udzielonej przez producenta, zgodnie z ust. 5.1. Zakres rękojmi obejmuje również dokonywanie napraw przedmiotu umowy.
- 5.3. Początkiem okresu gwarancyjnego dla Systemu oraz rękojmi jest dzień podpisania protokołu odbioru bez uwag, o którym mowa w ust. 2.3.
- 5.4. W przypadku nieprzystąpienia Wykonawcy na podstawie rękojmi do usunięcia wad lub nieusunięcia ich w terminach opisanych w załączniku nr 5, Zamawiający będzie miał prawo zlecić wykonanie prac objętych rękojmią innemu podmiotowi, w tym innemu autoryzowanemu przez producenta Systemu serwisowi na koszt (obciążając Wykonawcę kosztami takiego zastępczego wykonania) i na ryzyko Wykonawcy, na co Wykonawca niniejszym wyraża zgodę.
- 5.5. Wszelkie koszty związane z zapewnieniem obsługi w ramach rękojmi i gwarancji, a w szczególności: koszty dojazdu, transportu, montażu, demontażu, instalacji i konfiguracji ponosi odpowiednio Wykonawca lub producent.
- 5.6. Zgłoszenia wad Systemu będą przyjmowane:
  - 1) na podstawie rękojmi - przez Wykonawcę w formie wiadomości – email, wysyłanych na adres poczty elektronicznej wskazany w ust. 6.2; Wykonawca każdorazowo będzie potwierdzał Zamawiającemu fakt usunięcia wady Systemu na adres e-mail: informatycy@olsztyn.eu.
  - 2) na podstawie gwarancji – zgodnie z zasadami gwarancji określonymi przez producenta.
- 5.7. Okres gwarancji oraz rękojmi ulega każdorazowo przedłużeniu o czas od momentu zgłoszenia Systemu do wymiany, do momentu uzyskania możliwości ponownego korzystania z Systemu.

## **§ 6. ODPOWIEDZIALNOŚĆ**

- 6.1. W razie opóźnienia w dostarczeniu Systemu w stosunku do terminu, o którym mowa w ust. 2.1, Wykonawca zapłaci Zamawiającemu za każdy dzień opóźnienia karę umowną w wysokości 0,2 % ceny brutto określonej w ust. 4.1 umowy;
- 6.2. Uchybienie przez Wykonawcę terminowi naprawy lub wymiany Systemu określonego w załączniku nr 5, w ramach gwarancji lub rękojmi, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości:
  - 1) 250 zł za każdy dzień przekroczenia terminu – w odniesieniu do terminów przewidzianych w dniach;
  - 2) 100,00 zł za każdą godzinę przekroczenia terminu – w odniesieniu do terminów przewidzianych w godzinach.
- 6.3. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20 % ceny brutto określonej w ust. 4.1 w przypadku odstąpienia przez Zamawiającego od umowy z przyczyn leżących po stronie Wykonawcy.
- 6.4. W razie wykonania przez Zamawiającego prawa odstąpienia od umowy Zamawiający może dochodzić zarówno kary umownej przewidzianej w ust. 6.3 jak i innych kar umownych należnych do dnia odstąpienia od umowy.
- 6.5. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przewyższającego kary umowne na zasadach ogólnych.

## **§ 7.OSOBY ODPOWIEDZIALNE**

- 7.1. Osobami upoważnionymi do kierowania całością spraw związanych z realizacją umowy, w tym podpisania protokołu odbioru, o którym mowa w ust. 2.3, są:
- 1) w imieniu Zamawiającego:
    - (a) Dyrektor CIUWO lub osoba upoważniona przez Dyrektora CIUWO
  - 2) w imieniu Wykonawcy:
    - (a) .....
    - (b) .....
- 7.2. Osobami odpowiedzialnymi za realizację zapisów umowy, ze strony Zamawiającego, w zakresie zgłaszania uwag co do zgodności Systemu u z umową w razie stwierdzenia jego wad lub nieprawidłowości oraz w zakresie realizacji uprawnień reklamacyjnych lub gwarancyjnych, będą:
- 1) ..... (e-mail: .....);
  - 2) ..... (e-mail: .....).
- 7.3. Osobami odpowiedzialnymi za realizację zapisów umowy, ze strony Wykonawcy, będą:
- 1) .....
  - 2) .....
- 7.4. Zmiana osób wymienionych w ust. 7.1 - 7.3 w trakcie realizacji umowy wymaga poinformowania drugiej Strony w formie dokumentowej i nie stanowi zmiany umowy.
- 7.5. Strony zobowiązują się do kierowania wszelkiej korespondencji i oświadczeń, co do których umowa nie dopuszcza zachowania formy dokumentowej, na adresy stron wymienione w komparycji umowy, a w przypadku zmiany adresu, do niezwłocznego, pisemnego powiadomienia o tym fakcie drugiej Strony.
- 7.6. W przypadku braku powiadomienia, o którym mowa w ust. 7.5, doręczenie korespondencji na adres wskazany w komparycji umowy wywiera przewidziane prawem skutki prawne.

## **§ 8.ODSTĄPIENIE**

- 8.1. Zamawiający ma prawo odstąpić od umowy na zasadach określonych w kodeksie cywilnym dla umowy sprzedaży.
- 8.2. Zamawiający może odstąpić od umowy, bez wyznaczania dodatkowego terminu, w przypadku gdy opóźnienie w dostarczeniu Systemu - uchybienie terminowi wskazanemu w ust. 2.1. - przekroczy 10 dni.
- 8.3. Zamawiający ma prawo odstąpić od umowy na zasadach określonych w art. 145 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz.U. z 2018 r. poz. 1986, z późn. zm.). W przypadku odstąpienia od umowy na zasadach określonych w art. 145 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz.U. z 2018 r. poz. 1986, z późn. zm.) Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
- 8.4. Zamawiający ma prawo rozwiązać umowę na zasadach określonych w art. 145a ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz.U. z 2018 r. poz. 1986, z późn. zm.). W przypadku rozwiązania umowy na zasadach określonych w art. 145a ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn.: Dz.U. z 2018 r. poz. 1986, z późn. zm.) Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
- 8.5. Złożenie oświadczenia o odstąpieniu od umowy wymaga formy pisemnej pod rygorem nieważności.

## **§ 9.ZABEZPIECZENIE.**

- 9.1. Wykonawca przed zawarciem umowy ustanowił zabezpieczenie należytego wykonania umowy, w wysokości 10 % wynagrodzenia brutto, o którym mowa w ust. 4.1 w celu zabezpieczenia roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania umowy w formie ....<sup>5</sup>.
- 9.2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
- 9.3. Jeżeli zabezpieczenie wniesiono w pieniądzu, Zamawiający przechowa je na oprocentowanym rachunku bankowym. Zamawiający zwróci zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.
- 9.4. W trakcie realizacji umowy Wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w art. 148 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j.: Dz. U. z 2018 r., poz. 1986 z późn. zm.).
- 9.5. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.
- 9.6. W przypadku nieprzedłużenia lub niewniesienia nowego zabezpieczenia najpóźniej na 30 dni przed upływem terminu ważności dotychczasowego zabezpieczenia wniesionego w innej formie niż w pieniądzu, Zamawiający zmieni formę na zabezpieczenie w pieniądzu, poprzez wypłatę kwoty z dotychczasowego zabezpieczenia. Wypłata nastąpi nie później niż w ostatnim dniu ważności dotychczasowego zabezpieczenia.
- 9.7. Zamawiający zwraca 70% kwoty należytego zabezpieczenia umowy, w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należyte wykonane (tj. podpisania protokołu odbioru, o którym mowa w ust. 2.3, a 30% nie później niż w 15. dniu po upływie okresu rękojmi za wady.
- 9.8. Strony przewidują zmianę terminu realizacji umowy z powodu działania siły wyższej uniemożliwiającej realizację umowy w terminie określonym w ust. 2.1.
- 9.9. Zmiana terminu realizacji umowy dopuszczalna jest tylko o czas działania siły wyższej oraz o czas potrzebny do usunięcia skutków tego działania.
- 9.10. W przypadku stwierdzenia braku dostępności na rynku Systemu z przyczyn od Wykonawcy niezależnych, w szczególności wycofania oferowanego modelu z produkcji lub wprowadzenia zakazu importu lub eksportu danego modelu dopuszcza się, bez zmiany terminu realizacji, dostarczenie Systemu o cechach i parametrach nie gorszych niż zaproponowane w ofercie oraz zgodnych z parametrami technicznymi i użytkowymi określonymi w załączniku nr 1 do umowy. Zmiana nie wpływa na wysokość ceny należnej Wykonawcy z tytułu realizacji niniejszej umowy.

## **§ 10.PODWYKONAWCY**

---

<sup>5</sup> Należy uzupełnić zgodnie z wyborem przez Wykonawcę jednej lub kilku z następujących form zabezpieczenia:

1. pieniądź;
2. poręczenia bankowe lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
3. gwarancje bankowe;
4. gwarancje ubezpieczeniowe;
5. poręczenia udzielane przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

- 10.1. Wykonawca odpowiada wobec Zamawiającego za działania i zaniechania podwykonawców jak za swoje własne działania i zaniechania.
- 10.2. Wykonawca zapewnia, że podwykonawcy będą przestrzegać wszelkich postanowień umowy.
- 10.3. Wykonawca nie może powierzyć podwykonawcom do wykonania innych części przedmiotu umowy niż te, które wymienił w swojej ofercie, bez uprzedniej zmiany umowy z Zamawiającym w formie pisemnej.

#### **§ 11. POSTANOWIENIA KOŃCOWE**

- 11.1. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
- 11.2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy ustawy Prawo zamówień publicznych, Kodeksu cywilnego oraz inne odpowiednie przepisy powszechnie obowiązującego prawa.
- 11.3. Ewentualne spory powstałe w związku z wykonywaniem przedmiotu umowy będą rozpatrywane przez sądy powszechne właściwe miejscowo dla Zamawiającego.
- 11.4. Wykonawca bez uprzedniej pisemnej zgody Zamawiającego nie może dokonać przeniesienia wierzytelności wynikających z niniejszej umowy na osoby trzecie.
- 11.5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.
- 11.6. Następujące załączniki stanowią integralną część umowy:
  - Załącznik nr 1. – Szczegółowy opis przedmiotu zamówienia;
  - Załącznik nr 2. – Oferta Wykonawcy;
  - Załącznik nr 3. – Wzór protokołu odbioru;
  - Załącznik nr 4. – Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej.

**Zamawiający**

**Wykonawca**



## **Załącznik nr 1 SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

System WIFI powinien posiadać funkcjonalność podstawową obejmującą następujące elementy:

1. Punkty dostępowe (Access Point) – 50 sztuk
2. Kontroler
3. Aplikacja

Powyższe elementy podstawowe systemu muszą być zgodne z poniższym opisem przedmiotu zamówienia

### **1. PUNKT DOSTĘPOWY**

- 1) Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2 oraz 2.4GHz b/g/n
- 2) Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej
- 3) Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:
  - 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. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
- 4) Musi być zapewniona możliwość wspólnej konfiguracji punktów dostępowych połączonych w jedną sieć LAN w warstwie 2:
  - 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) Musi być zapewniona możliwość tworzenia klastra do 120 punktów dostępowych
- 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) Punkt dostępowy musi mieć wbudowany serwer DHCP
- 8) Punkt dostępowy musi mieć wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów
- 9) Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
  - a) EAP-TLS
  - b) PEAP-MSCHAPv2
  - c) PEAP-GTC
  - d) TTLS-MSCHAPv2
- 10) Musi istnieć możliwość obsługi uwierzytelniania RADIUS oraz LDAP w oparciu o zewnętrzne serwery tych usług.
- 11) Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID
- 12) Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN
- 13) Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:

- a) Portal wbudowany w punkt dostępowy, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania
  - b) Zewnętrzny portal WWW
- 14) Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT
- 15) Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne
- 16) 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
  - d) Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
  - e) Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz
  - f) Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac oraz starszych (802.11b/g)
  - g) Wsparcie dla 802.11d oraz 802.11h
  - h) Możliwość stworzenia profili czasowych w których dane ssid ma być rozgłaszane
- 17) Punkt dostępowy musi minimalizować zakłócenia częstotliwości sieci 3G/4G LTE
- 18) Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej, oraz jako dostęp do konsoli urządzenia
- 19) Obsługa roamingu klientów w warstwie 2
- 20) Obsługa monitoringu przez SNMP
- 21) Obsługa logowania na zewnętrznym serwerze SYSLOG
- 22) W system operacyjny punktu dostępowego musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
- 23) W system operacyjny punktu dostępowego musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
- 24) Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
- 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/s dla każdego radia
  - f) Szum tła dla każdego radia
  - g) Wyświetlanie logów systemowych
- 25) Punkt dostępowy musi posiadać 2 anteny dwuzakresowe do pracy w trybie 2x2:2 MU-MIMO, o zysku co najmniej 3,0 dBi dla 2,4 Ghz oraz co najmniej 5,5 dBi dla 5 Ghz.
- 26) Musi być zapewniona obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2
- 27) Musi być zapewniona praca punktu dostępowego w trybie MIMO 2X2:2
- 28) Specyfikacja radia 802.11a/n/ac wave 2
- a) Obsługiwane częstotliwości
    - 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) Obsługiwana technologia OFDM
  - c) Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
  - d) Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm
  - e) Prędkości transmisji:
    - 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a
    - MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n

- MCS0-MCS9, NSS = 1-4(6.5 Mbps do 867 Mbps) dla 802.11ac
- f) Obsługa HT – kanały 20/40MHz dla 802.11n
  - g) Obsługa VHT – kanały 20/40/80MHz dla 802.11ac
  - h) Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz
  - i) Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac
  - j) Wsparcie dla:
    - MRC (Maximal ratio combining)
    - CDD/CSD (Cyclic delay/shift diversity)
    - STBC (Space-time block coding)
    - LDPC (Low-density parity check)
    - Technologia TxBF
- 29) Specyfikacja radia 802.11b/g/n:
- a) Częstotliwość 2,400 ~2,4835
  - b) Technologia direct sequence spread spectrum (DSSS), OFDM
  - c) Typy modulacji – CCK, BPSK, QPSK, 16-QAM, 64-QAM
  - d) Moc transmisji konfigurowalna przez administratora
  - e) Prędkości transmisji:
    - 1,2,5.5,11 Mbps dla 802.11b
    - 6,9,12,18,24,36,48,54 Mbps dla 802.11g
- 30) Punkt dostępowy musi posiadać co najmniej:
- a) 1 interfejs 10/100/1000 Base-T
    - z funkcją PoE
    - zgodny ze standardem 802.3az Energy Efficient Ethernet
  - b) 1 interfejs konsoli RS-232
  - c) Moduł Bluetooth Low Energy (BLE) radio
    - Do 3 dBm mocy nadawczej (class2 ) oraz czułość -93 dBm
    - Zintegrowana antena uzysku do 4.5 dBi i kącie promieniowania 30 °
  - d) zasilanie 12V AC oraz PoE 48V DC zgodne z 802.3af
    - maksymalny pobór mocy 11 przy zasilaniu PoE
    - maksymalny pobór mocy 9 przy zasilaniu DC
  - e) przycisk przywracający konfigurację fabryczną
- 31) Parametry pracy punktu dostępowego:
- a) Temperatura otoczenia: 0-40 ° C
  - b) Wilgotność 10% - 90%
  - c) Znak CE
  - d) UL/IEC/EN 60950
  - e) EN 60601-1-1, EN60601-1-2
- 32) Punkt dostępowy musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac wave2
- 33) Urządzenie musi być dostarczone z zestawem do montażu wewnątrz budynków (na ścianie)
- 34) Każdy punkt dostępowy musi być objęty minimum 36 miesięczną gwarancją producenta obejmującą wszystkie elementy urządzenia zapewniającą dostawę sprawnego sprzętu na podmiannę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

## 2. Aplikacja

- 1) Licencja na Oprogramowanie musi pozwalać na zarządzaniem minimum 50 urządzeniami sieciowymi każdego typu (licencja nie może być ograniczona do jednego typu urządzeń, jeżeli zarządzanie danym typem urządzeń wymaga oddzielnego licencjonowania, muszą być one zaoferowane ponad wymagane minimum).
- 2) Aplikacja do Zarządzania i Monitoringu tego samego producenta co oferowane urządzenia WLAN
- 3) Aplikacja musi być możliwa do zainstalowania w środowisku wirtualnym VMware
- 4) Obsługa aplikacji poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW
- 5) Zarządzanie wszystkimi punktami dostępowymi AP oraz kontrolerami Sieci Radiowej będących przedmiotem tego samego postępowania
- 6) Licencja Aplikacji musi pozwalać na obsługę wszystkich niezbędnych urządzeń.
- 7) Aplikacja musi wspierać środowiska heterogenicznych, czyli możliwość zarządzania z wykorzystaniem SNMP urządzeniami sieciowymi różnych producentów
  - a) Automatyczne wykrywanie urządzeń
  - b) Bieżące monitorowanie stanu wszystkich podłączonych urządzeń
  - c) Funkcja automatycznej konfiguracji urządzeń sieci radiowej po podłączeniu się ich do sieci
  - d) Funkcja zbierania i wyświetlania informacji dotyczących pracujących w sieci urządzeń klienckich oraz możliwość ich wyszukania przy użyciu różnych parametrów takich jak:
    - i. system operacyjny
    - ii. typ urządzenia
    - iii. użytkowanego urządzenia sieci WLAN oraz danego SSID
  - e) Funkcja pełnej wizualizacji położenia urządzeń znajdujących się w sieci
  - f) Funkcja archiwizacji konfiguracji urządzeń
  - g) Konfiguracja zadań dla podłączonych urządzeń, w szczególności
    - i. automatyczna zmiana wersji oprogramowania urządzeń,
    - ii. ponowne uruchomienie urządzenia
    - iii. definiowanie przedziałów czasowych, w których dane SSID ma być rozgłaszane
  - h) Narzędzie ułatwiające planowanie radiowe dla sieci posiadające możliwość wizualizacji pokrycia radiowego
  - i) Funkcja tworzenia map pokrycia (tzw. Heat Map)
  - j) Panel zarządzający GUI umożliwiający wyświetlanie przynajmniej
    - i. Wykresu liczby zasocjowanych urządzeń klienckich
    - ii. Wykresu potencjalnej przepustowości urządzeń klienckich
    - iii. Wykresu stosunku sygnał do szumu (SNR) urządzeń klienckich
  - k) Funkcja automatycznego wykrycia urządzeń fałszywych, jego lokalizacji oraz ich ograniczenie np. poprzez rozłączenie urządzeń podłączonych do AP
  - l) Funkcja generowania ostrzeżeń i logów dotyczących wykrytych ataków w sieci bezprzewodowej
  - m) Funkcja generowania wiadomości email dla administratorów sieci (alerty, ostrzeżenia)
  - n) Funkcja definiowania poziomu dostępu dla administratorów z przypisanymi:
    - i. Rolami
    - ii. Segmentami sieci, do których uzyskuje się dostęp
  - o) Obsługa XMP API
  - p) Funkcja monitorowania jakości oraz ilości połączeń Unified Communication and Collaboration

- 8) Aplikacja musi być objęta minimum 36 miesięczną gwarancją (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 8x5xNBD na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

### **3. KONTROLER**

- 1) Kontroler musi zarządzać siecią bezprzewodową złożoną z 50 punktów dostępowych z możliwością rozbudowy do co najmniej 512 punktów dostępowych (Access Point)
- 2) Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall)
- 3) Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym.
- 4) Kontroler musi umożliwiać pracę w klastrze HA
- 5) Komunikacja kontrolera z innymi kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych.
- 6) Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania
- 7) Kontroler musi zapewniać centralne zarządzania licencjami, tzn. w architekturze sieci, w której występują więcej niż jeden kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom.
- 8) Kontroler musi posiadać następujące parametry sieciowe:
  - a) możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,
  - b) wsparcie dla sieci VLAN w tym również trunk 802.1q
  - c) wbudowany serwer DHCP
  - d) obsługa SNMPv2, SNMPv3
  - e) routing dynamiczny OSPF
- 9) Kontroler sieci WLAN musi obsługiwać co najmniej:
  - a) Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST, DES, 3DES, AES-CBC
  - b) Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze
  - c) Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit
  - d) Autoryzację dostępu użytkowników:
    - i. 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 support for EAP, RFC 3580, 3748, captive portal, 802.1X i MAC
    - ii. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia
    - iii. Wsparcie dla autoryzacji, minimum: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC
    - iv. Musi 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”
    - v. Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)

- vi. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym
- vii. 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.
- e) Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.
- f) Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu
- g) Kontroler musi zapewniać obsługę XML API do uwierzytelnienia
- 10) Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci:
  - a) Integracja jednoczesnej transmisji danych i głosu
  - b) Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p
  - c) Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming)
  - d) Musi umożliwiać ograniczanie pasma dla użytkownika oraz dla roli użytkownika
  - e) Musi umożliwiać ograniczenie pasma dla poszczególnych aplikacji
  - f) Musi umożliwiać ograniczenie pasma dla poszczególnych SSID
- 11) Kontroler musi umożliwiać integrację ze środowiskiem Microsoft Lync poprzez SDN API.
- 12) Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal)
- 13) Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona (interfejs) przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni)
- 14) Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:
  - 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
  - c) Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi
  - d) Rozkład ruchu pomiędzy różnymi punktami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma
  - e) Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie
  - f) Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b)
  - g) Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
  - h) Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w
- 15) Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności:
  - a) Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia
  - b) Kopiowanie (mirroring) sesji
  - c) Szczegółowe logi (per pakiet) do późniejszej analizy

- d) ALG (Application Layer gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP
  - e) Translacja źródłowa, docelowa adresów IP
  - f) Identyfikacja i blokowanie ataków DoS
  - g) Obsługa protokołu GRE
  - h) Deep packet inspection (DPI)
  - i) Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi
- 16) Kontroler musi umożliwiać rozbudowę o funkcjonalność WIDS/ WIPS, posiadającą co najmniej poniższe możliwości:
- a) Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.
  - b) Identyfikacja i możliwość blokowania sieci Adhoc
  - c) Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging
  - d) Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler
  - e) Identyfikacja błędów konfiguracji klientów WLAN
  - f) Identyfikacja podszywania się pod autoryzowane punkty dostępowe
- 17) 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 (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie).
- 18) Zarządzanie kontrolerem musi odbywać się poprzez co najmniej wszystkie następujące metody:
- a) interfejs przeglądarki Web (https),
  - b) linia komend przez SSH
  - c) dedykowany port konsoli.
- 19) Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA
- 20) Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi:
- a) Możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 512
  - b) Liczba jednocześnie obsługiwanych adresów MAC nie mniej niż 16000
  - c) Liczba aktywnych sesji zapory sieciowej nie mniej niż 2000000,
  - d) przepustowość nie mniej niż (duże pakiety) 20Gbps
  - e) Liczba obsługiwanych BSSID nie mniej niż 8192
  - f) Liczba jednoczesnych sesji IPSEC nie mniej niż 16000
  - g) Minimum 4 porty 10GBASE-X ze stykiem definiowanym przez SFP+. Obsadzone 2 wkładkami SFP+ 10Gb/s MM (zasięg nie mniej niż 220m).
  - h) Dołączone 2 patchcordsy 2 metrowe LC-LC MM klasy nie mniej niż OM3 oraz 2 patchcordsy 1-metrowe LC-LC MM klasy nie mniej niż OM3
  - i) Minimum 2 porty gigabitowe w standardzie 10/100/1000BaseT
  - j) Minimum 2 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT)
  - k) 1 interfejs konsoli (mini USB/RJ-45)
  - l) Minimum 1 port USB 2.0
  - m) Zużycie energii nie większe niż 120W
  - n) Pełna obsługa standardu 802.1Q – 4094 tagów sieci VLAN

- o) Dwa wbudowane (wewnętrzne, modułowe) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
- 21) Dla kontrolera wymagana zgodność z normami CE
  - 22) Kontroler musi być objęty minimum 36 miesięczną gwarancją (serwis) producenta obejmującą wszystkie elementy urządzenia (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie co najmniej 8x5 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
  - 23) Jeżeli to jakichkolwiek wymaganych funkcjonalności niezbędne jest dostarczenie dedykowanych licencji producenta to muszą one być udzielone na czas nieokreślony.
  - 24) W ramach realizacji przedmiotu umowy Wykonawca uruchomi i skonfiguruje kontroler z do współpracy i zarządzania 5 wskazanymi przez Zamawiającego punktami dostępowymi.



**OFERTA WYKONAWCY**

## WZÓR

## PROTOKÓŁ ODBIORU KOŃCOWEGO

do umowy nr \_\_\_\_\_ z dnia \_\_\_\_\_

| Odbierający:  |
|---|
| Gmina Olsztyn – Centrum Informatycznych Usług<br>Wspólnych Olsztyna, Pl. Jana Pawła II 1, 10-101<br>Olsztyn, NIP 739-384-70-26<br>(Zamawiający) |

| Przekazujący:                 |
|-------------------------------|
| _____<br>_____<br>(Wykonawca) |

Świadczenia polegające odbiorowi (przedmiot odbioru):

| Lp. | Świadczenia polegające odbiorowi (przedmiot odbioru): | Data odbioru                                     | Uwagi   |
|-----|---|--|---|
| 1.  | [Opis przedmiot odbioru zgodnie z umową]              | [Data dostarczenia świadczenia zgodnego z umową] | [Zastrzeżenia lub stwierdzenie zgodności świadczenia z umową] |
| 2.  |   |  |   |
| 3.  |   |  |   |

Przedmiot odbioru zostaje przyjęty bez zastrzeżeń

Z uwagi na zgłoszone uwagi w tabeli Zamawiający odmawia odbioru przedmiotu odbioru<sup>6</sup>

|  |
|--|
|  |
|  |

Dodatkowe uzasadnienie

[Dodatkowe uzasadnienie decyzji – jeśli dotyczy]

Dodatkowe ustalenia,

[Opis dodatkowych ustaleń – jeśli dotyczy]

Dodatkowe uwagi:

|                           |               |
|---------------------------|---------------|
| Przekazujący (Wykonawca): |               |
|                           | <i>podpis</i> |

| Zamawiający:    |  |            |  |
|-----------------|--|------------|--|
| Imię i nazwisko |  | Stanowisko |  |
| Data protokołu  |  | Podpis     |  |

<sup>6</sup> Należy zaznaczyć właściwy kwadrat



**OŚWIADCZENIE WYKONAWCY O AKCEPTACJI PRZESYŁANIA FAKTUR DROGĄ ELEKTRONICZNĄ**

Na podstawie art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174, z późn. zm.) **Zamawiający: Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna**; Pl. Jana Pawła II 1, 10-101 Olsztyn; NIP 739-384-70-26, akceptuje przesyłanie, w tym udostępnianie faktur, ich korekt oraz duplikatów w formie PDF za pośrednictwem poczty elektronicznej.

**Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna oświadcza, że:**

1. Faktury VAT i korekty faktur należy przysyłać na adres email: sekretariat@ciuwo.olsztyn.eu,
2. Tytuł wiadomości email musi zawierać wyrażenie: faktura/faktury lub korekta/korekty lub korygująca/korygujące lub duplikat/duplikaty
3. Faktury VAT i korekty faktur, Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna wysyła z adresu e-mail: sekretariat@ciuwo.olsztyn.eu.

Podpis Zamawiającego

**Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej**

Na podstawie art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174, z późn. zm.) akceptuję przesyłanie, w tym udostępnianie faktur, ich korekt oraz duplikatów w formie PDF za pośrednictwem poczty elektronicznej:

Nazwa firmy Wykonawcy:

Adres Wykonawcy:

Nr NIP Wykonawcy:

**Oświadczam, że:**

Faktury/korekty faktur/duplikaty faktur będę przysyłać do Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna z adresu e-mail:

Adres skrzynki nadawczej Wykonawcy:

Adresem właściwym do przesyłania faktur/ korekty faktur/duplikaty faktur przez Gminę Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna jest adres e-mail:

Adres skrzynki odbiorczej Wykonawcy:

Podpis Wykonawcy

**INFORMACJE DODATKOWE:**

1. Faktury wraz ze wszystkimi załącznikami muszą być zapisane w formie PDF oraz załączone bezpośrednio do wiadomości e-mail.
2. Faktury i załączniki nie mogą być kompresowane i zaszyfrowane.
3. Skrzynka odbiorcza Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna – email: [sekretariat@ciuwo.olsztyn.eu](mailto:sekretariat@ciuwo.olsztyn.eu) jest obsługiwana automatycznie. Fakturę uważa się za doręczoną w momencie wpływu na skrzynkę odbiorczą Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna.
4. Wskazane powyżej adresy skrzynek pocztowych Zamawiającego i Wykonawcy są jedynymi właściwymi adresami stanowiącymi gwarancję pochodzenia faktury.