Kraków, dnia 05.10.2021 r.

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Tryb podstawowy na podstawie art. 275 pkt 1 ustawy Prawo Zamówień Publicznych

Dostawa sprzętu i oprogramowania informatycznego II

Zamawiający:

Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny

30-418 Kraków, ul. Zakopiańska 73

ZATWIERDZAM:

**1. Nazwa oraz adres Zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania**

Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny

30-418 Kraków, ul. Zakopiańska 73

tel. (12) 26 18 324/111, faks (12) 26 60 870

NIP 675-000-00-88 REGON 387116932

Adres strony internetowej: https://kit.lukasiewicz.gov.pl/

Adres poczty elektronicznej: sekretariat@kit.lukasiewicz.gov.pl

https://platformazakupowa.pl/pn/kit.lukasiewicz – strona internetowa prowadzonego postępowania

**2. Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia**

https://platformazakupowa.pl/pn/kit.lukasiewicz– strona internetowa prowadzonego postępowania

**3. Tryb udzielenia zamówienia**

Postępowanie jest prowadzone w trybie podstawowym na podstawie art. 275 pkt 1 ustawy Pzp - postępowanie o wartości mniejszej niż progi unijne.

*Gdziekolwiek w niniejszej specyfikacji przywołana jest ustawa lub przepis bez dalszego uszczegółowienia to należy przez to rozumieć Ustawę Prawo Zamówień Publicznych (nazywaną również w SWZ – „ustawa Pzp”) . W sytuacji zacytowania wprost w SWZ określonego przepisu prawa przytoczona jest jego literalna treść. Słowa przekreślone w treści cytatu oznaczają, że występują one w literalnie zacytowanym tekście źródłowym lecz Zamawiający wykreślił je w SWZ w celu zwiększenia przejrzystości tekstu jako niemające zastosowania w niniejszym postępowaniu.*

**4. Informacja, czy zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji**

Zamawiający nie przewiduje możliwości prowadzenia negocjacji.

**5. Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest: **Dostawa sprzętu i oprogramowania informatycznego:**

Część I – Zakup i dostawa przełączników sieciowych, bezprzewodowych punktów dostępowych, kontrolera punktów bezprzewodowych, oprogramowania zarządzającego wraz z systemem NAC

Część II - Zakup i dostawa monitora komputerowego - 1 szt.

Część III - Zakup i dostawa laptopów - 10 szt.

Cześć IV - Zakup usługi zapewnienia wsparcia producenta dla oprogramowania VMWare posiadanego przez Zamawiającego

Część I: CPV: 32424000-1, 32427000-2

Część II: CPV: 30231300-0

Część III: CPV: 30213100-6, 30237410-6

Część IV: CPV: 72591000-4

Postępowanie oznaczone jest znakiem **ZP/12/21**. Wykonawcy winni we wszelkich kontaktach   
z Zamawiającym powoływać się na wyżej podane oznaczenie.

Szczegółowy opis przedmiotu zamówienia zawiera **załącznik nr 3** będący integralną częścią SWZ. Gdziekolwiek w Specyfikacji Warunków Zamówienia przywołane są normy, lub nazwy własne lub znaki towarowe lub patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę Zamawiający dopuszcza rozwiązania równoważne.

**6. Termin wykonania zamówienia**

 Część I: do 29 grudnia 2021 r. wraz z dostarczeniem Zamawiającemu faktury – podanie daty dziennej wynika z konieczności rozliczenia zadania jeszcze w tym roku kalendarzowym

Część II: 3 tygodnie od podpisania umowy

Część III: 2 tygodnie od podpisania umowy

Część IV: 7 dni od podpisania umowy

**7. Projektowane postanowienia umowy w sprawie zamówienia publicznego**

1. Zamawiający wymaga, aby Wykonawca zawarł umowę w sprawie zamówienia publicznego wg wzoru stanowiącego **załącznik nr 2** do SWZ.

2. Zamawiający prześle umowę Wykonawcy, którego oferta została wybrana za najkorzystniejszą albo zaprosi go do swojej siedziby, celem podpisania umowy.

**8. Informacja o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej**

1. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem Platformy Zakupowej (dalej jako „Platforma”) pod adresem: <https://platformazakupowa.pl>

2. Komunikacja między Zamawiającym a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane są w formie elektronicznej za pośrednictwem Platformy i formularza „wyślij wiadomość”. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformy poprzez kliknięcie przycisku „wyślij wiadomość” po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.

3. Zamawiający z Wykonawcami będzie przekazywał informacje w formie elektronicznej za pośrednictwem Platformy. Informacje dotyczące odpowiedzi na pytania, zmiany SWZ, zmiany terminu składania i otwarcia ofert zamawiający będzie zamieszczał na platformie.

Korespondencja której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca będzie przekazywana w formie elektronicznej za pośrednictwem Platformy do tego konkretnego Wykonawcy.

4. Niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na Platformie Zakupowej, tj.:

a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,

b) komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje.

c) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10 0.,

d) włączona obsługa JavaScript,

e) zainstalowany program Adobe Acrobat Reader, lub inny obsługujący format plików .pdf.

5. Zalecane formaty przesyłanych danych, tj. plików o wielkości do 75 MB. - Zalecany

format: pdf. Zamawiający dopuszcza również inne powszechnie stosowane formaty takie

jak na przykład: doc, docx, xls, jpg, zip, 7Z.

6. Zalecany format kwalifikowanego podpisu elektronicznego:

a) dokumenty w formacie pdf zaleca się podpisywać formatem PAdES;

b) dopuszcza się podpisanie dokumentów w formacie innym niż .pdf, wtedy zaleca się użyć

formatu XAdES.

7. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z Platformy Zakupowej, określone w Regulaminie zamieszczonym na stronie internetowej pod adresem <https://platformazakupowa.pl/strona/1-regulamin> w zakładce „Regulamin" oraz uznaje go za wiążący.

8. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem <https://platformazakupowa.pl/strona/45-instrukcje>

**9. Informacja o sposobie komunikowania się zamawiającego z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej**

Zamawiający będzie się porozumiewał przy użyciu środków komunikacji elektronicznej.

**10. Wskazanie osób uprawnionych do komunikowania się z wykonawcami**

Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami w sprawie przetargu jest:

Marek Dziewit – sprawy formalne – tel. 693289533,

Elżbieta Tomczyk – sprawy merytoryczne dotyczące przedmiotu zamówienia - tel. 12 26 18 187

**11. Termin związania ofertą**

### Wykonawca jest związany ofertą do dnia 13.11.2021 r.

**12. Opis sposobu przygotowywania i składania ofert oraz innych oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu**

1. Oferta powinna być:
   1. sporządzona na podstawie załączników niniejszej SWZ w języku polskim.
   2. złożona w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym za pośrednictwem Platformy Zakupowej Zamawiającego

2. Zamawiający informuje Wykonawców o treści art. 18 ust. 3 ustawy Pzp który brzmi:

„Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649), jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5.”

3. Wykonawca jest zobligowany do złożenia ofert, oświadczeń, informacji oraz dokumentów w sposób zgodny z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie, zwanego dalej w niniejszym punkcie SWZ – Rozporządzeniem.

Zgodnie z § 2 ust 1 i 2 Rozporządzenia:

1. ~~Wnioski o dopuszczenie do udziału w postępowaniu lub konkursie, wnioski, o których mowa w art. 371 ust. 3 ustawy~~, oferty, ~~prace konkursowe~~, oświadczenia, o których mowa w art. 125 ust. 1 ustawy, podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust. 3 ustawy, zwane dalej „zobowiązaniem podmiotu udostępniającego zasoby”, przedmiotowe środki dowodowe, pełnomocnictwo, ~~dokumenty, o których mowa w art. 94 ust. 2 ustawy~~, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568, 695, 1517 i 2320), ~~z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy~~, z uwzględnieniem rodzaju przekazywanych danych.

2. Informacje, oświadczenia lub dokumenty, inne niż określone w ust. 1, przekazywane w postępowaniu ~~lub w konkursie~~, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej, o których mowa w § 3 ust. 1 (tj. platformy zakupowej Zamawiającego).

Zgodnie z § 4 ust 1 Rozporządzenia:

1. W przypadku gdy dokumenty elektroniczne w postępowaniu ~~lub konkursie~~, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.

Zgodnie z § 5 Rozporządzenia:

Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski. Tłumaczenie nie jest wymagane, jeżeli zamawiający wyraził zgodę, w przypadkach, o których mowa w art. 20 ust. 3 ustawy.

Zgodnie z § 6 Rozporządzenia:

1. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, ~~w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy~~, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument.

2. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, ~~w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy~~, lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone ~~kwalifikowanym podpisem elektronicznym, a~~ w przypadku postępowań ~~lub konkursów~~ o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.

3. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w ust. 2, dokonuje w przypadku:

1) podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;

2) przedmiotowych środków dowodowych – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzie-lenie zamówienia;

3) innych dokumentów, ~~w tym dokumentów, o których mowa w art. 94 ust. 2 ustawy~~ – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.

4. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w ust. 2, może dokonać również notariusz.

5. Przez cyfrowe odwzorowanie, o którym mowa w ust. 2–4 oraz § 7 ust. 2–4, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.

Zgodnie z § 7 Rozporządzenia:

1. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, ~~dokumenty, o których mowa w art. 94 ust. 2 ustawy~~, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się ~~kwalifikowanym podpisem elektronicznym, a~~ w przypadku postępowań ~~lub konkursów~~ o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

2. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w ust. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, ~~dokumenty, o których mowa w art. 94 ust. 2 ustawy~~, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone ~~kwalifikowanym podpisem elektronicznym, a~~ w przypadku postępowań ~~lub konkursów~~, o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.

3. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w ust. 2, dokonuje w przypadku:

1) podmiotowych środków dowodowych – odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;

2) przedmiotowego środka dowodowego, ~~dokumentu, o którym mowa w art. 94 ust. 2 ustawy~~, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;

3) pełnomocnictwa – mocodawca.

4. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w ust. 2, może dokonać również notariusz.

Zgodnie z § 8 Rozporządzenia:

W przypadku przekazywania w postępowaniu ~~lub konkursie~~ dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty ~~kwalifikowanym podpisem elektronicznym, a~~ w przypadku postępowań ~~lub konkursów~~ o wartości mniejszej niż progi unijne, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

Zgodnie z § 10 Rozporządzenia:

Dokumenty elektroniczne w postępowaniu ~~lub w konkursie~~ spełniają łącznie następujące wymagania:

1) są utrwalone w sposób umożliwiający ich wielokrotne odczytanie, zapisanie i powielenie, a także przekazanie przy użyciu środków komunikacji elektronicznej lub na informatycznym nośniku danych;

2) umożliwiają prezentację treści w postaci elektronicznej, w szczególności przez wyświetlenie tej treści na monitorze ekranowym;

3) umożliwiają prezentację treści w postaci papierowej, w szczególności za pomocą wydruku;

4) zawierają dane w układzie niepozostawiającym wątpliwości co do treści i kontekstu zapisanych informacji.

4. Wykonawca, za pośrednictwem Platformy może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem <https://platformazakupowa.pl/strona/45-instrukcje>

5. Każdy z Wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.

6. Ceny oferty muszą zawierać wszystkie koszty jakie musi ponieść Wykonawca, aby zrealizować zamówienie z

najwyższą starannością oraz ewentualne rabaty.

7. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem <https://platformazakupowa.pl/strona/45-instrukcje>

**13. Kształt oferty. Wykaz dokumentów składających się na ofertę oraz oświadczeń i dokumentów które należy złożyć wraz z ofertą.**

1. Zamawiający wymaga od Wykonawcy złożenia:

a) pełnomocnictwa do podpisania oferty, jeżeli osobą podpisującą nie jest osoba upoważniona na podstawie wypisu z Krajowego Rejestru Sądowego  lub zaświadczenia o wpisie do centralnej ewidencji i informacji o działalności gospodarczej. Jeżeli dołączone do oferty ww. pełnomocnictwo będzie w formie kopii, Zamawiający wymaga, aby jego zgodność z oryginałem poświadczyła osoba wymieniona w rejestrze, która jest wskazana, jako upoważniona do reprezentowania Wykonawcy lub notariusz,

b) oświadczenia Wykonawcy w zakresie niepodlegania wykluczeniu z postępowania na podstawie art. 125 ust. 1 ustawy Pzp, wg **załącznika nr 1** do SWZ,

c) wypełniony formularz ofertowy – wg **załącznika nr 4** do SWZ.

Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W powyższym przypadku wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców, którzy wspólnie ubiegają się o udzielenie zamówienia. Jeżeli oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zostanie wybrana, zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych wykonawców.

W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie o którym mowa w pkt b składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

**14. Przedmiotowe środki dowodowe**

Zamawiający nie wymaga przedmiotowych środków dowodowych.

**15. Podmiotowe środki dowodowe**

Zamawiający nie wymaga podmiotowych środków dowodowych. Wykonawca zobowiązany jest jedynie do złożenia oświadczenia o którym mowa w pkt 13.1.b) SWZ.

**16. Sposób oraz termin składania ofert**

1.Ofertę wraz z wymaganymi dokumentami należy zamieścić na Platformie pod adresem: <https://platformazakupowa.pl/pn/kit.lukasiewicz> **do dnia 15.10.2021 r. do godz. 09:10** w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.

2. Po wypełnieniu **Formularza** składania ofertyi załadowaniu wszystkich wymaganych załączników należy kliknąć przycisk **„Przejdź do podsumowania”.**

3. W procesie składania oferty za pośrednictwem platformy Wykonawca może złożyć podpis w następujący sposób:

- bezpośrednio na dokumencie przesłanym do Platformy lub/i

- dla całego pakietu dokumentów w kroku 2 **Formularza** składania oferty(po kliknięciu w przycisk **„Przejdź do podsumowania”**.

4.Za datę przekazania oferty przyjmuje się datę jej przekazania w systemie (platformie) wraz z wgraniem paczki w formacie XML w drugim kroku składania oferty poprzez kliknięcie przycisku “ **Złóż ofertę**” i wyświetlaniu komunikatu, że oferta została złożona.

5.Szczegółowa instrukcja dla Wykonawców dotycząca złożenia oferty znajduje się na stronie internetowej pod adresami: <https://platformazakupowa.pl/strona/1-regulamin> oraz <https://platformazakupowa.pl/strona/45-instrukcje>

**17. Termin otwarcia ofert**

1. Otwarcie ofert nastąpi **w dniu 15.10.2021 r., o godzinie 09:20** za pośrednictwem Platformy Zakupowej Zamawiającego w siedzibie Zamawiającego: Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny ul. Zakopiańska 73, 30-418 Kraków w Budynku „BLT” (wejście od strony ul. Zbrojarzy) I piętro - sala konferencyjna.

2. Informację z otwarcia ofert Zamawiający udostępni na Platformie Zakupowej niniejszego postępowania w zakładce „Komunikaty”.

**18. Warunki udziału w postępowaniu**

Zamawiający nie stawia warunków udziału w postępowaniu.

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 108 ust. 1 ustawy Pzp. Podstawy wykluczenia podane w punkcie poniżej.

**19. Podstawy wykluczenia Wykonawcy z postępowania**

Podstawy wykluczenia Wykonawcy zostały podane w art. 108 ust. 1 ustawy Prawo zamówień publicznych. Art. 108 ust. 1 ustawy Prawo zamówień publicznych stanowi:

1. Z postępowania o udzielenie zamówienia wyklucza się wykonawcę:

1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,

b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,

c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,

d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego po-chodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

f) pracy małoletnich cudzoziemców powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,

h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

– lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) 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 1;

3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o do-puszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

Zgodnie z art 110 ustawy Pzp:

1. Wykonawca może zostać wykluczony przez zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

2. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub ~~art. 109 ust. 1 pkt 2‒5 i 7‒10~~, jeżeli udowodni zamawiającemu, że spełnił łącznie następujące przesłanki:

1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;

2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;

3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:

a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,

b) zreorganizował personel,

c) wdrożył system sprawozdawczości i kontroli,

d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,

e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

3. Zamawiający ocenia, czy podjęte przez wykonawcę czynności, o których mowa w ust. 2, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w ust. 2, nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza wykonawcę.

Zgodnie z art. 111 ustawy Pzp:

Wykluczenie wykonawcy następuje:

1) w przypadkach, o których mowa w art. 108 ust. 1 pkt 1 lit. a–g i pkt 2, na okres 5 lat od dnia uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia;

2) w przypadkach, o których mowa w:

a) art. 108 ust. 1 pkt 1 lit. h i pkt 2, gdy osoba, o której mowa w tych przepisach, została skazana za przestępstwo wymienione w art. 108 ust. 1 pkt 1 lit. h,

b) ~~art. 109 ust. 1 pkt 2 i 3~~

~~‒ na okres 3 lat od dnia uprawomocnienia się odpowiednio wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, wydania ostatecznej decyzji lub zaistnienia zdarzenia będącego podstawą wykluczenia, chyba że w wyroku lub decyzji został określony inny okres wykluczenia~~;

3) w przypadku, o którym mowa w art. 108 ust. 1 pkt 4, na okres, na jaki został prawomocnie orzeczony zakaz ubiegania się o zamówienia publiczne;

4) w przypadkach, o których mowa w art. 108 ust. 1 pkt 5, ~~art. 109 ust. 1 pkt 4, 5, 7 i 9~~, na okres 3 lat od zaistnienia zdarzenia będącego podstawą wykluczenia;

5) w przypadku, o którym mowa w ~~art. 109 ust. 1 pkt 8~~, na okres 2 lat od zaistnienia zdarzenia będącego podstawą wykluczenia;

6) w przypadku, o którym mowa w ~~art. 109 ust. 1 pkt 10~~, na okres roku od zaistnienia zdarzenia będącego podstawą wykluczenia.;

7) w przypadkach, o których mowa w art. 108 ust. 1 pkt 6 i ~~art. 109 ust. 1 pkt 6~~, w postępowaniu o udzielenie zamówienia, w którym zaistniało zdarzenie będące podstawą wykluczenia.

**20. Sposób obliczenia ceny**

1. Wykonawca zobowiązany jest do podania cen w sposób określony w załączniku nr 4 SWZ.

**UWAGA:**

1. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2018 r. poz. 2174, z późn. zm.15)), dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.

2. W ofercie, o której mowa w punkcie powyżej wykonawca ma obowiązek:

1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;

2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;

3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;

4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

**21. Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert**

I . Zamawiający przy wyborze ofert będzie kierował się kryteriami podanymi poniższej - **dla części** I:

**60 %** - cena (C) – 60 pkt

Punktacja:

C = R1 x Cmin / Cb

Cmin – cena oferty najtańszej

Cb – cena oferty badanej

R1 – znaczenie procentowe kryterium Cena

**15%** - dodatkowa funkcja analityki (D) – 15 pkt

tj. oprogramowanie do zarządzania zapewnia realizację funkcji analityki obejmującą co najmniej:  
• System zarządzania musi posiadać przy współpracy z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej  
• Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.  
• Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.  
• System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos  
• System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.  
• Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.  
• System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.  
• System Analityki musi zapewniać możliwość tworzenia raportów.  
• System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.

Punktacja:

TAK – 15 pkt

NIE – 0 pkt  
  
**10 %** - obsługa więcej niż 1000 urządzeń klienckich (adresów MAC) – (E) – 10 pkt

oprogramowanie musi zostać dostarczone z odpowiednimi licencjami

Punktacja:

TAK – 10 pkt

NIE – 0 pkt  
  
**15 %** - integracja z systemami innych producentów oprogramowania do zarządzania – (F) – 15 pkt  
• System zarządzania posiada wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów: Palo Alto, Fortinet, Checkpoint

• Możliwość integracji systemu kontroli tożsamości z systemami firewall co najmniej z następującymi producentami: Palo Alto, Fortinet, Checkpoint

Punktacja:

TAK – 15 pkt

NIE – 0 pkt

Zamawiający wybierze ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w SIWZ. Za najkorzystniejszą uznana zostanie ta z ocenianych ofert, która uzyska maksymalną ocenę punktową (W) wg poniższego wzoru:

**W = C+D+E+F**

II. Zamawiający przy wyborze ofert będzie kierował się kryteriami podanymi w poniższej tabeli - **dla części II,III i IV**:

|  |  |  |  |
| --- | --- | --- | --- |
| ***L.p.*** | **Kryterium** | ***Znaczenie procentowe kryterium (Rj)*** | ***Maksymalna ilość punktów, jakie może otrzymać oferta za dane kryterium*** |
| 1. | Cena | C = 100% | 100 punktów |

Zamawiający wybierze ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w SIWZ. Za najkorzystniejszą uznana zostanie ta z ocenianych ofert, która uzyska maksymalną ocenę punktową wg poniższego wzoru.

**C = R1 x Cmin / Cb**

**Cmin – cena oferty najtańszej**

**Cb – cena oferty badanej**

**R1 – znaczenie procentowe kryterium Cena**

**22. Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty**

**w celu zawarcia umowy w sprawie zamówienia publicznego**

Zamawiający prześle umowę do Wykonawcy, którego oferta została wybrana za najkorzystniejszą albo zaprosi go do swojej siedziby celem podpisania umowy.

**23. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy**

Zamawiający informuje, iż Wykonawcy przysługują środki ochrony prawnej opisane w dziale IX ustawy Prawo Zamówień Publicznych.

Środki ochrony prawnej przysługują wykonawcy, oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy.

Odwołanie przysługuje na:

1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

2) zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy;

3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.

1. Odwołanie wnosi się do Prezesa Izby.

2. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.

2. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.

3. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

Odwołanie wnosi się w terminie:

a) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

b) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.

Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów za-mówienia na stronie internetowej.

Odwołanie w przypadkach innych niż określone powyżej wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

Odwołanie zawiera:

1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);

2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;

3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;

4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku – numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;

5) określenie przedmiotu zamówienia;

6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych albo publikacji w Dzienniku Urzędowym Unii Europejskiej;

7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzeniapostępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;

8) zwięzłe przedstawienie zarzutów;

9) żądanie co do sposobu rozstrzygnięcia odwołania;

10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;

11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;

12) wykaz załączników.

2. Do odwołania dołącza się:

1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;

2) dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;

3) dokument potwierdzający umocowanie do reprezentowania odwołującego.

**24. Opis części zamówienia, jeżeli zamawiający dopuszcza składanie ofert częściowych.**

Zamawiający dopuszcza składanie ofert częściowych na podane w załącznikach 3 i 4 części zamówienia. Wykonawca może złożyć ofertę na jedną lub więcej części zamówienia.

**25. Liczba części zamówienia, na którą wykonawca może złożyć ofertę.**

Brak ograniczeń.

**26. Informacja dotyczące ofert wariantowych.**

Zamawiający nie dopuszcza składania ofert wariantowych.

**27. Wymagania w zakresie zatrudnienia na podstawie stosunku pracy.**

Nie dotyczy

**28. Wymagania w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2.**

Nie dotyczy

**29. Informacja o zastrzeżeniu możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94, jeżeli zamawiający przewiduje takie wymagania.**

Nie dotyczy

**30. Wymagania dotyczące wadium, w tym jego kwota.**

Zamawiający nie wymaga wniesienia wadium.

**31. Informacja o przewidywanych zamówieniach, o których mowa w art. 214 ust. 1 pkt 7 i 8**

Zamawiający nie przewiduje zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8

**32. Informacje dotyczące przeprowadzenia przez wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2**

Nie dotyczy

**33. Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między zamawiającym a wykonawcą.**

Nie dotyczy

**34. Informacje dotyczące zwrotu kosztów udziału w postępowaniu.**

Nie dotyczy

**35. Informację o obowiązku osobistego wykonania przez wykonawcę kluczowych zadań.**

Nie dotyczy

**36. Maksymalna liczba wykonawców, z którymi zamawiający zawrze umowę ramową.**

Nie dotyczy

**37. Informacje o przewidywanym wyborze najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230.**

Nie dotyczy

**38. Wymóg lub możliwość złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93**

Nie dotyczy

**39. Informacje dotyczące zabezpieczenia należytego wykonania umowy.**

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

**40. Klauzula informacyjna z art. 13 RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego.**

Mając na uwadze zapisy art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, zwanym dalej „RODO”, poniżej podajemy informacje i zasady przetwarzania danych osobowych przez Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny w Krakowie.

**Administrator danych**

Administratorem Pani/Pana (Wykonawcy) danych osobowych jest **Sieć Badawcza Łukasiewicz –** **Krakowski** **Instytut Technologiczny** w Krakowie (zwany dalej: Instytut lub Zamawiający) z siedzibą ul. Zakopiańska 73 30-418 Kraków, adres e-mail: sekretariat@kit.lukasiewicz.gov.pl nr tel.: **12 26 18 324**

**Inspektor Ochrony Danych**

We wszelkich sprawach dotyczących przetwarzania danych osobowych przez Instytut można kontaktować się   
z wyznaczonym w tym celu Inspektorem Ochrony Danych, adres email: daneosobowe@kit.lukasiewicz.gov.pl lub osobiście w siedzibie Instytutu.

**Cel przetwarzania danych osobowych i podstawa prawna przetwarzania danych:**

Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w związku z przepisami ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych, dalej „ustawa Pzp" w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn.: **ZP/12/21 Dostawa sprzętu i oprogramowania informatycznego II**

- znak sprawy: **ZP/12/21** prowadzonym w trybie podstawowym

**Odbiorcy danych**

Odbiorcami Państwa danych osobowych są lub mogą być:

* 1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o ustawę Pzp;
  2. podmioty serwisujące urządzenia Instytutu za pośrednictwem których przetwarzane są Państwa dane osobowe;
  3. podmioty dostarczające i utrzymujące oprogramowanie wykorzystywane w celu przetwarzania danych osobowych Wykonawców, osób reprezentujących i pracowników Wykonawcy;
  4. podmioty świadczące na rzecz Instytutu usługi niezbędne do ewentualnego wykonania zawieranej z Państwem umowy – jeżeli zawarta z Państwem umowa wymaga ich udziału np. firmy kurierskie za pośrednictwem, których może być prowadzona z Państwem korespondencja.
  5. podmioty, którym przekazuje się dokumentację dla celów niszczenia po zakończonym okresie przechowywania;

Pani/Pana dane osobowe nie będą przekazywane do państw znajdujących się poza Europejskim Obszarem Gospodarczym i nie będą przekazywane do organizacji międzynarodowych.

**Okres, przez który dane będą przetwarzane**

Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy.

**Realizacja praw osób, których dane dotyczą**

Posiada Pani/Pan:

* prawo dostępu do danych osobowych Pani/Pana dotyczących (na podstawie art. 15 RODO);
* prawo do sprostowania Pani/Pana danych osobowych (na podstawie art. 16 RODO)\*;
* prawo żądania (na podstawie art. 18 RODO) od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO\*\*;
* prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa w przypadku uznania, że przetwarzanie przez Instytut Pani/Pana danych osobowych narusza przepisy RODO.

W celu wykonania praw wymienionych powyżej należy skierować żądanie na adres email: daneosobowe@kit.lukasiewicz.gov.pl, pisemnie na adres siedziby Instytutu lub osobiście w siedzibie Instytutu. Przed realizacją Państwa uprawnień Instytut musi potwierdzić Państwa tożsamość w sposób indywidualnie dostosowany do danego żądania.

Nie przysługuje Pani/Panu:

* w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
* prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
* na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

**Informacja o wymogu podania danych**

Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych wynikają z ustawy Pzp.

**Decyzje podejmowane w sposób zautomatyzowany**

Instytut nie będzie stosował wobec Pani/Pana zautomatyzowanego podejmowania decyzji, w tym profilowania.

Wyjaśnienie:

\* Skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

\*\* Prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

***26.*** ***Załączniki***

1. Załącznik nr 1 – oświadczenie Wykonawcy w zakresie niepodlegania wykluczeniu z

postępowania

2.Załącznik nr 2 – Wzór umowy

3. Załącznik nr 3 – Opis przedmiotu zamówienia

4. Załącznik nr 4 – Formularz ofertowy

ZATWIERDZAM

**Załącznik nr 1 do SWZ**

**Zamawiający:**

**Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny**

**30-418 Kraków, ul. Zakopiańska 73**

**Wykonawca:**

………………..………………………………………

*(pełna nazwa/firma)*

………………..………………………………………

*(adres)*

………………..………………………………………

*tel./fax)*

*.............................................................*

*w zależności od podmiotu: NIP/PESEL,KRS/CEiDG)*

reprezentowany przez:

………………….............................……

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie wykonawcy**

**składane na podstawie art. 125 ust. 1 ustawy**

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

Na potrzeby postępowania o udzielenie zamówienia publicznego: **Dostawa sprzętu i oprogramowania informatycznego II,** prowadzonego przez Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny*,* oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY ( właściwe zaznaczyć i jeśli dotyczy wypełnić puste pole ):**

* Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
* Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …………. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia art. 108 ust. 1 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, podjąłem następujące środki naprawcze: …………………………….………………………………………………………………………………………………………………………………………………..…………………………………………………………………………………………..…………………...........…………………………………………

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne   
i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

**OŚWIADCZENIE DOTYCZĄCE DEFINICJI PRZEDSIĘBIORSTWA:**

Oświadczam, że zgodnie z ROZPORZĄDZENIEM KOMISJI (UE) NR 651/2014 z dnia 17 czerwca 2014 r. jestem:

* - mikro przedsiębiorstwem
* - małym przedsiębiorstwem
* - średnim przedsiebiorstwem
* - dużym przedsiębiorstwem

\* właściwe zaznaczyć

**Załącznik nr 2 do SWZ**

**UMOWA ZP/…../21 (dla części nr 1,2,3 )**

zawarta w Krakowie, w dniu ……………….. r. pomiędzy:

Siecią Badawczą Łukasiewicz – Krakowskim Instytutem Technologicznym z siedzibą w Krakowie, 30-418 Kraków, ul. Zakopiańska 73, wpisanym do Krajowego Rejestru Sądowego przez Sąd Rejonowy dla Krakowa-Śródmieście, XI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000861401, NIP: 675-000-00-88, REGON 387116932 , reprezentowanym przez:

……………………………………………………………………………………………………………………….

zwanym w dalszej części umowy **„Zamawiającym”**

a

………………………………………………………………………………………………………………………

reprezentowanym przez:

……………………………………………………………………………………………………………………..

zwanym w dalszej części umowy **„Wykonawcą”**

*W wyniku udzielenia zamówienia publicznego w trybie podstawowym o szacunkowej wartości* ***zamówienia poniżej 214 000 euro*** *– postępowanie nr* ***ZP/12/21*** *o następującej treści:*

**§ 1**

**Przedmiot umowy.**

1. Na warunkach określonych niniejszą umową, Wykonawca sprzedaje Zamawiającemu ……….., zwane dalej przedmiotem zamówienia.
2. Parametry techniczne przedmiotu zamówienia, warunki licencji na oprogramowanie wchodzące w zakres przedmiotu zamówienia oraz warunki gwarancji określa załącznik nr 1 do umowy (zał. nr ……. do SIWZ) oraz oferta Wykonawcy stanowiąca załącznik nr 2 do umowy.
3. Wykonawca zobowiązuje się również do dostarczenia przedmiotu zamówienia na adres wskazany przez Zamawiającego.
4. Wykonawca zobowiązany jest do podpisania i przestrzegania Załącznika nr 3 - zobowiązania do zachowania poufności
5. Wykonawca zapewnia serwis gwarancyjny w zakresie wszelkich składowych przedmiotu umowy oraz nieodpłatne przeglądy serwisowe w okresie gwarancyjnym. Wykonawca, w ramach serwisu gwarancyjnego, zapewni także wsparcie techniczne obejmujące pomoc w weryfikacji, zgłaszaniu oraz rozwiązywaniu problemów wynikających z funkcjonowania całości przedmiotu umowy.
6. Jakakolwiek usterka lub awaria, która wystąpi w okresie gwarancji zostanie usunięta przez Wykonawcę na jego koszt i ryzyko, przy uwzględnieniu niezbędnych składowych działań zmierzających do usunięcia wady lub usterki w postaci: dojazdu serwisu na miejsce przedmiotu umowy, ewentualnego transportu sprzętu do serwisu, oraz wszelkich kosztów wymienianych części i robocizny, w tym - wszelkich, pozostałych działań zmierzających do skutecznego wypełnienia przez Wykonawcę jego zobowiązań z tytułu gwarancji. Powyższe dotyczy także każdej sytuacji zniszczenia przez którąkolwiek ze składowych przedmiotu niniejszej umowy infrastruktury Zamawiającego, w tym funkcjonujących u Zamawiającego systemów programów komputerowych i innych systemów informatycznych. W sytuacji opisanej w zdaniu uprzednim, Wykonawca przejmuje na siebie wszelkie ciężary i ryzyko naprawienia zaistniałych u Zamawiającego szkód do pełnej ich wysokości, w tym zobowiązuje się przejąć i świadczyć na rzecz Zamawiającego zobowiązania jakie wynikają z gwarancji posiadanych przez Zamawiającego na infrastrukturę, programy komputerowe oraz systemy informatyczne.
7. Zgłoszenia ewentualnych wad i usterek Zamawiający będzie dokonywał faksem lub mailem z zastrzeżeniem, że potwierdzenie prawidłowej transmisji faksu lub maila stanowi dowód skutecznego zgłoszenia przez Zamawiającego wady lub usterki. Reakcja Wykonawcy będzie polegać na: potwierdzeniu otrzymania zgłoszenia (przy pomocy faksu lub maila), przybyciu do siedziby Zamawiającego celem dokonania oględzin ewentualnej awarii lub usterki. Zamawiający dopuszcza również realizację wsparcia technicznego lub usunięcia usterki poprzez zdalny dostęp do systemu. Wsparcie techniczne realizowane będzie telefonicznie lub pocztę e-mail.
8. Stwierdzona w okresie gwarancji wada lub usterka którejkolwiek z części składowych przedmiotu umowy kwalifikuje tę część składową do naprawy lub wymiany na nową, na koszt i ryzyko Wykonawcy. Wykonawca w takim przypadku jest zobowiązany dostarczyć Zamawiającemu naprawiony (w pełni sprawny) lub nowy, wolny od wad przedmiot umowy w zakresie wszelkich jego składowych podlegających naprawie lub wymianie, o takich samych co zamówiony parametrach, w terminie do 10 dni roboczych, licząc od daty dokonania przez Zamawiającego zgłoszenia stosownego żądania faksem lub mailem (z zastrzeżeniem, iż potwierdzenie prawidłowej transmisji faksu lub maila stanowi dowód dokonania skutecznego zgłoszenia przez Zamawiającego). Czasookres naprawy którejkolwiek ze składowych przedmiotu umowy powoduje przedłużenie czasu obowiązywania udzielonej pierwotnie gwarancji w zakresie tej składowej o czas niefunkcjonowania przedmiotu umowy na skutek wad i usterek.
9. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień z tytułu rękojmi.

**§ 2**

**Cena i warunki wykonania umowy**

* + - 1. Za wykonanie obowiązków określonych w § 1 umowy, Zamawiający zapłaci Wykonawcy kwotę ........................... brutto (słownie: ...................................... ). Kwota ta obejmuje cenę przedmiotu zamówienia wraz z kosztem transportu i wszelkimi obowiązkami wynikającymi z zawartej umowy, w tym kosztami licencji potrzebnych do korzystania z oprogramowania wchodzącego w zakres przedmiotu zamówienia.
      2. Umowa zostanie zrealizowana najpóźniej w terminie ……………………..
      3. O terminie dostawy przedmiotu zamówienia Wykonawca zawiadomi Zamawiającego z trzydniowym wyprzedzeniem. Wykonawca dostarczy Zamawiającemu przedmiot zamówienia na własny koszt i ryzyko. W szczególności, Wykonawca ponosi odpowiedzialność za utratę, zniszczenie lub uszkodzenie przedmiotu zamówienia w trakcie transportu lub montażu.
      4. Wykonawca udziela gwarancji na zasadach określonych w załączniku nr 1 do umowy(zał. nr …….….. do SIWZ)

**§ 3**

**Odbiór i warunki płatności**.

* + - 1. Odbiór odbędzie się po dostarczeniu przedmiotu zamówienia, w wyniku którego zostanie sporządzony przez przedstawicieli obu stron protokół, sporządzony w formie pisemnej i podpisany przez obie strony.
      2. Zapłata należności nastąpi przelewem wterminie 30 dni od daty otrzymania faktury, wystawionej w oparciu o protokół odbioru, o którym mowa w ust.1, z którego wynika, że Zamawiający nie zgłasza zastrzeżeń.
      3. Brak uwag do protokołu, nie uchybia prawu Zamawiającego do wysuwania roszczeń z tytułu nienależytego wykonania umowy, a w szczególności z tytułu rękojmi, w przypadku późniejszego wykrycia lub ujawnienia wad.

**§ 4**

**Odpowiedzialność odszkodowawcza.**

* + - 1. W razie nieterminowego wykonania umowy Zamawiający może naliczyć karę umowną z tego tytułu w wysokości 0.2% kwoty określonej w § 2 ust. 1 za każdy dzień zwłoki, licząc od następnego dnia po terminie wskazanym w § 2 ust. 2.
      2. Jeśli zwłoka w wykonaniu umowy przekracza 30 dni, Zamawiający może od umowy odstąpić, naliczając z tego tytułu karę umowną w wysokości 20 % kwoty określonej w § 2 ust. 1, niezależnie od kary umownej naliczonej na podstawie ust. 1.
      3. W razie nieterminowego wykonywania obowiązków wynikających z rękojmi lub z udzielonej gwarancji, Zamawiający może naliczyć karę umowną z tego tytułu w wysokości 0.2% ceny określonej w § 2 ust. 1 za każdy dzień zwłoki, licząc od następnego dnia po wyznaczonym terminie.
      4. Strony dopuszczają możliwość dochodzenia odszkodowania uzupełniającego na zasadach ogólnych ponad zastrzeżone kary umowne.
      5. Maksymalna wysokość kar umownych naliczonych na podstawie niniejszej umowy nie może przekroczyć 30% kwoty podanej w § 2.1

**§ 5**

**Postanowienia dodatkowe**

Ewentualne koszty związane z zawarciem i realizacją umowy niewymienione w umowie obciążają Wykonawcę.

Wykonawca nie może dokonać cesji wierzytelności wynikających z niniejszej umowy bez zgody Zamawiającego wyrażonej w formie pisemnej, pod rygorem nieważności.

**§ 6**

**Postanowienia końcowe.**

* + - 1. W sprawach nieuregulowanych niniejszą umową zastosowanie mieć będą przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
      2. Wszelkie spory wynikające z niniejszej umowy lub związane z jej wykonaniem rozstrzygać będzie sąd powszechny właściwy ze względu na siedzibę Zamawiającego.
      3. Załączniki stanowią integralną część umowy:

a. załącznik nr 1- OPZ- Parametry techniczne przedmiotu umowy, gwarancja,

b. załącznik nr 2 - Oferta Wykonawcy

c. załącznik nr 3 - zobowiązanie do zachowania poufności

d. załącznik nr 4 – Informacja dla pracowników Wykonawcy – Wykonawca zobowiązany jest przekazać niniejszą informację osobom, których dane przekazał Zamawiającemu w związku z realizacją niniejszej umowy.

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

***Wykonawca* *Zamawiający***

**…………………. ……………………**

**UMOWA ZP/…../21 (dla części nr 4 )**

zawarta w Krakowie, w dniu ……………….. r. pomiędzy:

Siecią Badawczą Łukasiewicz – Krakowskim Instytutem Technologicznym z siedzibą w Krakowie, 30-418 Kraków, ul. Zakopiańska 73, wpisanym do Krajowego Rejestru Sądowego przez Sąd Rejonowy dla Krakowa-Śródmieście, XI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000861401, NIP: 675-000-00-88, REGON 387116932 , reprezentowanym przez:

……………………………………………………………………………………………………………………….

zwanym w dalszej części umowy **„Zamawiającym”**

a

………………………………………………………………………………………………………………………

reprezentowanym przez:

……………………………………………………………………………………………………………………..

zwanym w dalszej części umowy **„Wykonawcą”**

*W wyniku udzielenia zamówienia publicznego w trybie podstawowym o szacunkowej wartości* ***zamówienia poniżej 214 000 euro*** *– postępowanie nr* ***ZP/12/21*** *o następującej treści:*

**§ 1**

**Przedmiot umowy.**

1. Na warunkach określonych niniejszą umową, Wykonawca sprzedaje Zamawiającemu ……….., zwane dalej przedmiotem zamówienia.
2. Przedmiot zamówienia określa załącznik nr 1 do umowy (zał. nr ……. do SIWZ) oraz oferta Wykonawcy stanowiąca załącznik nr 2 do umowy.
3. Wykonawca zobowiązuje się również do dostarczenia przedmiotu zamówienia na adres wskazany przez Zamawiającego.
4. Wykonawca zobowiązany jest do podpisania i przestrzegania Załącznika nr 3 - zobowiązania do zachowania poufności

**§ 2**

**Cena i warunki wykonania umowy**

1. Za wykonanie obowiązków określonych w § 1 umowy, Zamawiający zapłaci Wykonawcy kwotę ........................... brutto (słownie: ...................................... ). Kwota ta obejmuje cenę przedmiotu zamówienia wraz z kosztem transportu i wszelkimi obowiązkami wynikającymi z zawartej umowy.
2. Umowa zostanie zrealizowana najpóźniej w terminie ……………………..

**§ 3**

**Odbiór i warunki płatności**.

1. Odbiór odbędzie się po dostarczeniu przedmiotu zamówienia, w wyniku którego zostanie sporządzony przez przedstawicieli obu stron protokół, sporządzony w formie pisemnej i podpisany przez obie strony.
2. Zapłata należności nastąpi przelewem wterminie 30 dni od daty otrzymania faktury, wystawionej w oparciu o protokół odbioru, o którym mowa w ust.1, z którego wynika, że Zamawiający nie zgłasza zastrzeżeń.
3. Brak uwag do protokołu, nie uchybia prawu Zamawiającego do wysuwania roszczeń z tytułu nienależytego wykonania umowy, a w szczególności z tytułu rękojmi, w przypadku późniejszego wykrycia lub ujawnienia wad.

**§ 4**

**Odpowiedzialność odszkodowawcza.**

1. W razie nieterminowego wykonania umowy Zamawiający może naliczyć karę umowną z tego tytułu w wysokości 0.2% kwoty określonej w § 2 ust. 1 za każdy dzień zwłoki, licząc od następnego dnia po terminie wskazanym w § 2 ust. 2.
2. Jeśli zwłoka w wykonaniu umowy przekracza 30 dni, Zamawiający może od umowy odstąpić, naliczając z tego tytułu karę umowną w wysokości 20 % kwoty określonej w § 2 ust. 1, niezależnie od kary umownej naliczonej na podstawie ust. 1.
3. Strony dopuszczają możliwość dochodzenia odszkodowania uzupełniającego na zasadach ogólnych ponad zastrzeżone kary umowne.
4. Maksymalna wysokość kar umownych naliczanych na podstawie niniejszej umowy nie może przekroczyc 30% kwoty wynagrodzenia, o którym mowa w § 2.1.

**§ 5**

**Postanowienia dodatkowe**

1. Ewentualne koszty związane z zawarciem i realizacją umowy niewymienione w umowie obciążają Wykonawcę.
2. Wykonawca nie może dokonać cesji wierzytelności wynikających z niniejszej umowy bez zgody Zamawiającego wyrażonej w formie pisemnej, pod rygorem nieważności.

**§ 6**

**Postanowienia końcowe.**

1. W sprawach nieuregulowanych niniejszą umową zastosowanie mieć będą przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
2. Wszelkie spory wynikające z niniejszej umowy lub związane z jej wykonaniem rozstrzygać będzie sąd powszechny właściwy ze względu na siedzibę Zamawiającego.
3. Załączniki stanowią integralną część umowy:

a. załącznik nr 1- OPZ- Parametry techniczne przedmiotu umowy

b. załącznik nr 2 - Oferta Wykonawcy

c. załącznik nr 3 - zobowiązanie do zachowania poufności

d. załącznik nr 4 – Informacja dla pracowników Wykonawcy – Wykonawca zobowiązany jest przekazać niniejszą informację osobom, których dane przekazał Zamawiającemu w związku z realizacją niniejszej umowy.

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

***Wykonawca* *Zamawiający***

**…………………. ……………………**

Załącznik 3 do umowy

**ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI**

Ja, <*imię, nazwisko*>, zwany dalej Przyjmującym zobowiązanie, wykonując zadania w imieniu <*nazwa podmiotu – strony umowy*>, polegające na <*zakres działań i odwołanie do umowy*> zobowiązuję się do zachowania w tajemnicy i ochrony informacji poufnych, Administratorem których jest Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny w Krakowie, zwany dalej: Instytut, które pozyskałem w związku z zadaniami wynikającymi z podjętej współpracy/umowy.

Przyjmuję do wiadomości, że:

1. Informacją poufną jest każda informacja za wyjątkiem informacji wyraźnie oznaczonej jako ogólnie dostępna, informacji udostępnionej publicznie lub informacji klasyfikowanej jako informacja publiczna.

Szczególnie informacjami poufnymi są: dane medyczne, dane osobowe, informacje o środkach, środowisku i metodach pracy Instytutu, w tym informacje o procesach, politykach, procedurach i instrukcjach. Sposób przetwarzania ww. informacji nie wpływa na klasyfikację informacji jako poufnych.

2. Zobowiązanie do zachowania w tajemnicy i ochrony informacji poufnych rozumiane jest jako:

a. Nie ujawnianie stronom trzecim informacji poufnych oraz zachowanie staranności w działaniu w celu utrzymania ww. informacji w tajemnicy.

b. Nie kopiowanie i niepowielanie informacji poufnych w celach innych niż realizacja zadań będących przedmiotem współpracy/umowy.

c. Spełnienie ustawowych wymagań związanych z dostępem do danych (jeżeli zakres świadczonej usługi wiąże się z dostępem do danych osobowych: uczestnictwo w szkoleniu z tego zakresu oraz uzyskanie upoważnienia dostępu do tych danych przed realizacją usługi na rzecz Instytutu)[[1]](#footnote-1).

d. Zwrot Instytutowi informacji poufnych łącznie z kopiami oraz usunięcie tych informacji z wszystkich systemów przetwarzania i przechowywania danych Przyjmującego zobowiązanie – za wyjątkiem sytuacji, w których przechowywanie kopii danych poufnych przez Przyjmującego zobowiązanie wynika z umowy i/lub odrębnych przepisów prawa.

3. Zobowiązanie do zachowania poufności jest wyłączone w stosunku do informacji poufnych, które muszą zostać ujawnione z tytułu orzeczenia sądu lub decyzji administracyjnej wydanej na podstawie obowiązujących przepisów prawa, pod warunkiem, że Przyjmujący zobowiązanie jest stroną

w postępowaniu przed sądem lub stroną decyzji administracyjnej zobowiązującej do wyjawienia informacji otrzymanych na podstawie niniejszego zobowiązania.

4. Zobowiązanie do zachowania poufności jest wyłączone w stosunku do osób, które wskaże na piśmie Instytut.

5. Dane osobowe Przyjmującego zobowiązanie są przetwarzane przez Instytut z tytułu realizacji umowy między stronami, której stroną jest ww. Dane osobowe Przyjmującego zobowiązanie nie będą udostępniane, a Przyjmujący zobowiązanie ma prawo do wglądu do tych danych i żądania korekty, w sytuacji, kiedy dane będą niezgodne ze stanem faktycznym. Zakres przetwarzanych danych jest ograniczony do danych wymienionych w umowie oraz danych potwierdzających możliwość jej realizacji przez Przyjmujący zobowiązanie.

………………………………………………………………………

Data i Podpis przyjmującego zobowiązanie

(Zobowiązanie obowiązuje od daty jego złożenia

**Załącznik nr 4 do umowy**

**Obowiązek informacyjny   
(informacja dla pracowników Wykonawcy)**

Zgodnie z art.14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 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 (dalej: RODO), uprzejmie informujemy:

1) Administratorem Pani/Pana danych osobowych jest: **Sieć Badawcza Łukasiewicz –** **Krakowski** **Instytut Technologiczny** w Krakowie (zwany dalej: Instytut lub Zamawiający) z siedzibą ul. Zakopiańska 73 30-418 Kraków, adres e-mail: sekretariat@kit.lukasiewicz.gov.pl nr tel.: **12 26 18 32**

2) Z Inspektorem Ochrony Danych można się skontaktować poprzez adres email: daneosobowe@kit.lukasiewicz.gov.pl lub osobiście w siedzibie Instytutu we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z ich przetwarzaniem.

3) Przetwarzanie Pani/Pana danych osobowych odbywa się w celu realizacji umowy………………………………………………………………………………………….., na podstawie art.6 ust.1 lit. f RODO, zgodnie z którego treścią dopuszcza się przetwarzanie danych osobowych jeśli jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.

4) Dane osobowe będą udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na podstawie przepisów obowiązującego prawa oraz podmiotom współpracującym   
z Instytutem w zakresie realizacji rozwiązań technicznych i organizacyjnych, dostawcom usług (np. pocztowych, teleinformatycznych).

5) Pani/Pana dane osobowe przechowywane będą przez okres wymagany przepisami prawa,   
a następnie usuwane lub anonimizowane.

6) Każdemu, kogo dane dotyczą przysługuje prawo: dostępu do swoich danych, sprostowania (poprawiania) swoich danych, ograniczenia przetwarzania danych, wniesienia sprzeciwu wobec przetwarzania danych oraz wniesienia skargi do Prezesa UODO (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa).

7) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.  
  
8) Pani/Pana dane osobowe nie będą wykorzystywane do podejmowania zautomatyzowanych decyzji, a także nie będą wykorzystywane w celu profilowania.

**Załącznik nr 3 do SWZ**

**Opis przedmiotu zamówienia**

**Część I**

**Zakup i dostawa przełączników sieciowych, bezprzewodowych punktów dostępowych, kontrolera punktów bezprzewodowych, oprogramowania zarządzającego wraz z systemem NAC**

1. **Przełącznik Typ 1 – 2 szt.**
2. Przełącznik posiadający:
   1. 48 portów 1G/10G/25G SFP28
   2. 8 portów 40G/100G QSFP28
3. Wysokość urządzenia 1RU
4. Dedykowany port do zarządzania przełącznikiem „poza pasmem”
5. Dedykowany port konsoli szeregowej RJ45
6. Nieblokująca architektura wyposażona w chipset o przepustowości min. 4 Tb/s
7. Prędkość przełączania pakietów min. 970 Mpp/s
8. Przełącznik musi być wyposażony w dwa zasilacze, które umożliwiają realizację redundancji zasilania z możliwością ich wymiany w czasie pracy przełącznika
9. Przełącznik musi być wyposażony w redundantny system wentylacji z chłodzeniem przód-tył
10. Przełącznik musi mieć możliwość pracy w trybie tradycyjnym, czyli przełączanym/routowanym, ale również z wykorzystaniem technologii Fabric lub równoważnej (wirtualizacja usług warstwy drugiej i trzeciej wraz z obsługą multicast)
11. Tablica MAC adresów min. 160 tys. wpisów
12. Pamięć operacyjna: min. 8 GB pamięci DRAM
13. Pamięć flash/SSD: min. 128 GB pamięci Flash/SSD
14. Obsługa IEEE 802.1Q oraz min. 4 tys. aktywnych sieci VLAN
15. Wsparcie dla ramek Jumbo Frame 9600 bajtów
16. Wsparcie protokołów STP, RSTP oraz MSTP
17. Wsparcie dla min. 12 instancji MSTP – IEEE 802.1s
18. Wsparcie dla obługi MLAG (Multi Chassis Link Aggregation) – możliwość dołączenia innych przełączników lub urządzeń z wykorzystaniem standardowego połączenia Link Aggregation IEEE 802.3ad do dwóch różnych przełączników obsługujących MLAG
19. Możliwość „wirtualizacji” połączenia kontrolnego dla MLAG w ramach rozwiązania Fabric lub równoważnego
20. Obsługa min. 56 grup łączy typu Link Aggregation.
21. Obsługa Link Aggregation umożliwiająca zgrupowanie min. 8 portów w jednym łączu
22. Obsługa Link Aggregation wraz z obsługą LACP zgodna z IEEE 802.1AX

**Wymagania Layer 3**

1. Obsługa min. 32 tys. wpisów w tablicy ARP
2. Możliwość konfiguracji statycznych wpisów ARP
3. Obsługa protokołów routingu
   1. RIPv2 oraz RIPng
   2. OSPFv2 oraz OSPFv3
   3. BGP oraz BGPv6
4. Obsługa min. 512 interfejsów IP dla IPv4 oraz IPv6
5. Sprzętowa tablica routingu o pojemności min. 15 tys. wpisów dla IPv4 oraz 7 tys. wpisów dla IPv6
6. Obsługa balansowania ruchu ECMP
7. Obsługa redundancji routingu VRRPv3 dla IPv4 oraz IPv6 – min. 500 instancji
8. Obsługa UDP Forwarding / Obsługa DHCP Relay dla IPv4 oraz IPv6
9. Wsparcie min. 24 instancji VRF
10. Możliwość uruchomienia protokołów dynamicznego routingu w ramach serwisu L3 uruchomionego w ramach Fabric lub technologii równoważnej

**Wsparcie Multicast**

1. Obsługa IGMPv1, IGMPv2 oraz IGMPv3
2. Obsługa IGMP Snooping
3. Obsługa min. 4000 interfejsów IGMP
4. Obsługa protokołu routing Multicast PIM oraz PIM-SSM
5. Wsparcie multicast w rozwiązaniu Fabric lub równoważnym

**Bezpieczeństwo**

1. Obsługa DHCP snooping
2. Obsługa Dynamic ARP Inspection
3. Obsługa MAC Security
4. Obsługa IEEE 802.1x

**Wsparcie wirtualizacji – Fabric lub równoważne**

1. Wsparcie dla standardu IEEE 802.1aq / RFC 6329 Shortest Path Bridging
2. Wsparcie dla standardu IEEE 802.1ah Provider Backbone Bridging
3. Wsparcie dla standardu IEEE 802.1ag Connectivity Fault Management
4. Wsparcie mechanizmu kontroli usług pomiędzy różnymi IS-IS Area – przepuszczania lub blokowanie wskazanych serwisów L2 i L3 pomiędzy różnymi obszarami sieci
5. Wsparcie mechanizmu kontroli usług pomiędzy różnymi IS-IS Area
6. Wbudowane mechanizmy automatycznej konfiguracji Fabric lub technologii równoważnej – tworzenie nowej konfiguracji jak i dodawanie kolejnych urządzeń do Fabric lub technologii równoważnej
7. Obsługa min. 100 tys. MAC w ramach szkieletu Fabric lub technologii równoważnej
8. Obsługa min. 500 urządzeń w ramach Fabric lub technologii równoważnej
9. Obsługa min. 4000 serwisów L2 w ramach Fabric lub technologii równoważnej
10. Obsługa multicast w ramach serwisów L2
11. Obsługa 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
12. Wsparcie Remote Mirroring w ramach Fabric lub technologii równoważnej
13. Wsparcie mechanizmów rozszerzenia sieci Fabric lub równoważnej na inne lokalizacje poprzez dostępną sieć IP
14. Obsługa VXLAN

**Wsparcie telemetrii**

1. Sprzętowo wspomagana obsługa IPFIX w z prędkością łącza (ang. line-rate)
2. Obsługa wykrywania aplikacji działających w sieci na warstiwe 7 modelu OSI
3. Obsługa sFlow

**Zarządzania i inne**

1. Wsparcie zarządzania poprzez protokół SNMPv3
2. Obsługa SSHv2
3. Obsługa NTPv4
4. Zarządzanie poprzez przeglądarkę www i protokół HTTPS
5. Obsługa LLDP oraz LLDP-MED – IEEE 802.1AB
6. Obsługa RADIUS
7. Obsługa TACACS+
8. Obsługa SYSLOG
9. Możliwość uruchomienia na przełączniku dodatkowych maszyn wirtualnych – możliwość rozszerzenia poprzez licencję
10. **Przełącznik Typ 2 – 1 szt.**
11. Przełącznik wyposażony w 24 porty 10/100/1000BASE-T
12. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
13. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
14. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
15. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
16. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
17. Wysokość urządzenia 1U montowana w standardowym 19” Rack
18. Przełącznik musi posiadać dwa zasilacze 230V, które umożliwiają uzyskanie redundancji zasilania. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
19. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
20. Porty stakujące, w przypadku niewykorzystania ich do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty SFP+ z przepustowością 10 Gb/s
21. Możliwość łączenia do 8 przełączników w stos
22. Nieblokująca architektura o wydajności przełączania min. 208 Gb/s
23. Szybkość przełączania min. 154 Milionów pakietów na sekundę
24. Temperatura pracy przełącznika w zakresie min. 0o do 50o C
25. Tablica MAC adresów min. 32 tys.
26. Pamięć operacyjna: min. 1 GB pamięci DRAM
27. Pamięć flash: min. 1 GB pamięci Flash
28. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
29. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
30. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
31. Obsługa Q-in-Q IEEE 802.1ad
32. Obsługa Quality of Service
    1. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
    2. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
    3. 8 kolejek priorytetów na każdym porcie wyjściowym
    4. Obsługa kolejek Strict Priority
    5. Obsługa kolejek Weighted Round Robin
    6. Obsługa WRED (Weighted Random Early Detection)
33. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
34. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
35. Obsługa CDPv2 z obsługą Voice VLAN
36. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
37. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
38. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
39. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
40. Możliwość monitorowania zajętości CPU oraz pamięci
41. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
42. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
43. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
44. Dedykowany port konsoli szeregowej RJ45
45. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 - forwarding
2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
   1. RIP v1/v2
   2. OSPFv2 - możliwość rozszerzenia przez licencje
   3. BGPv4 - możliwość rozszerzenia przez licencje
   4. IS-IS - możliwość rozszerzenia przez licencje
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 - forwarding
2. Pojemność tabeli routingu min. 6 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
   1. RIPng
   2. OSPF v3 – możliwość rozszerzenia przez licencje
   3. BGPv4 – możliwość rozszerzenia przez licencje
   4. IS-IS – możliwość rozszerzenia przez licencje
5. Obsługa 6to4 (RFC 3056)
6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
7. Obsłgua MLDv2 (Multicast Listener Discovery version 2)
8. Policy Based Routing dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączanie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa PIM-SM
4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
6. Obsługa Multicast VLAN Registration - MVR
7. Obsługa IGMP v1 - RFC 1112
8. Obsługa IGMP v2 - RFC 2236
9. Obsługa IGMP v3 - RFC 3376
10. Obsługa IGMP v1/v2/v3 snooping
11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

**Bezpieczeństwo**

1. Obsługa logowania do sieci Network Login
   1. IEEE 802.1x based Network Login
   2. MAC based Network Login
   3. Web-based Network Login
2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
7. Obsługa Guest VLAN dla IEEE 802.1x
8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
10. Obsługa TACACS+ (RFC 1492)
11. Obsługa RADIUS Authentication (RFC 2138)
12. Obsługa RADIUS Accounting (RFC 2139)
13. RADIUS per-command Authentication
14. Obsługa RADIUS over TLS (RadSec) – RFC 6614
15. Bezpieczeństwo MAC adresów
16. ograniczenie liczby MAC adresów na porcie
17. zatrzaśnięcie MAC adresu na porcie
18. możliwość wpisania statycznych MAC adresów na port/vlan
19. Możliwość wyłączenia MAC learning
20. Zabezpieczenie przełącznika przed atakami DoS
    1. Networks Ingress Filtering RFC 2267
    2. SYN Attack Protection
    3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
21. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    1. Adres MAC źródłowy i docelowy plus maska
    2. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    3. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    4. Numery portów źródłowych i docelowych TCP, UDP
    5. Zakresy portów źródłowych i docelowych TCP, UDP
    6. Identyfikator sieci VLAN - VLAN ID
    7. Quality of Service IEEE 802.1p oraz DiffServ
    8. Flagi TCP
    9. Obsługa fragmentów
22. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
23. Możliwość konfiguracji min. 8 000 reguł na wejściu i 1 000 reguł na wyjściu
24. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
25. Obsługa bezpiecznego transferu plików SCP/SFTP
26. Obsługa DHCP Option 82
27. Obsługa IP Security – Trusted DHCP Server
28. Obsługa IP Security – DHCP Snooping and Guard
29. Obsługa IP Security - Gratuitous ARP Protection
30. Obsługa IP Security – DHCP Secured ARP/ARP Validation
31. Obsługa IP Security – IP Source guard
32. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
33. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

**Bezpieczeństwo sieciowe**

1. Możliwość konfiguracji portu głównego i zapasowego
2. Obsługa redundancji routingu VRRP
3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa ERPS / G.8032
8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
10. Obsługa LACP w ramach MLAG

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP lub NTP
2. Zarządzanie przez SNMP v1/v2/v3
3. Zarządzanie przez przeglądarkę WWW – protokół http i https
4. Możliwość zarządzania przez protokół XML
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)
13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

**Inne**

1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
3. Wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
4. Obsługa skryptów CLI
5. Obsługa funkcji TCL/Tk w skryptach CLI
6. Obsługa skryptów Python
7. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
8. Możliwość rozbudowy przełącznika o „wyniesione” porty (urządzenia) zarządzane z przełącznika – przykładowo zamiast prostych niezarządzalnych 8 portowych przełączników, urządzenie zarządzalne z przełącznika nadrzędnego.
9. Możliwość uruchamiania skryptów
   1. Ręcznie
   2. O określonym czasie lub co wskazany okres czasu
   3. Na podstawie wpisów w logu systemowym
10. **Przełącznik Typ 3 – 6 szt.**
11. Przełącznik wyposażony w 24 porty PoE+ 10/100/1000BASE-T
12. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
13. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
14. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
15. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
16. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
17. Wysokość urządzenia 1U montowana w standardowym 19” Rack
18. Przełącznik musi posiadać dwa zasilacze 230V, które umożliwiają uzyskanie redundancji zasilania. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
19. PoE+ zgodne ze standardem IEEE 802.3at.
20. Budżet mocy dla PoE+ min. 380W z jednego i 740W z dwóch zasilaczy.
21. Możliwość konfiguracji priorytetów wyłączenia PoE+ w przypadku braku budżetu mocy wynikającego np. z uszkodzenia pojedynczego zasilacza.
22. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
23. Porty stakujące, w przypadku niewykorzystania ich do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty SFP+ z przepustowością 10 Gb/s
24. Możliwość łączenia do 8 przełączników w stos
25. Nieblokująca architektura o wydajności przełączania min. 208 Gb/s
26. Szybkość przełączania min. 154 Milionów pakietów na sekundę
27. Temperatura pracy przełącznika w zakresie min. 0o do 50o C
28. Tablica MAC adresów min. 32 tys.
29. Pamięć operacyjna: min. 1 GB pamięci DRAM
30. Pamięć flash: min. 1 GB pamięci Flash
31. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
32. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
33. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
34. Obsługa Q-in-Q IEEE 802.1ad
35. Obsługa Quality of Service
    1. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
    2. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
    3. 8 kolejek priorytetów na każdym porcie wyjściowym
    4. Obsługa kolejek Strict Priority
    5. Obsługa kolejek Weighted Round Robin
    6. Obsługa WRED (Weighted Random Early Detection)
36. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
37. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
38. Obsługa CDPv2 z obsługą Voice VLAN
39. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
40. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
41. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
42. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
43. Możliwość monitorowania zajętości CPU oraz pamięci
44. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
45. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
46. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
47. Dedykowany port konsoli szeregowej RJ45
48. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 - forwarding
2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
   1. RIP v1/v2
   2. OSPFv2 - możliwość rozszerzenia przez licencje
   3. BGPv4 - możliwość rozszerzenia przez licencje
   4. IS-IS - możliwość rozszerzenia przez licencje
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 - forwarding
2. Pojemność tabeli routingu min. 6 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
   1. RIPng
   2. OSPF v3 – możliwość rozszerzenia przez licencje
   3. BGPv4 – możliwość rozszerzenia przez licencje
   4. IS-IS – możliwość rozszerzenia przez licencje
5. Obsługa 6to4 (RFC 3056)
6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
7. Obsłgua MLDv2 (Multicast Listener Discovery version 2)
8. Policy Based Routing dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączanie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa PIM-SM
4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
6. Obsługa Multicast VLAN Registration - MVR
7. Obsługa IGMP v1 - RFC 1112
8. Obsługa IGMP v2 - RFC 2236
9. Obsługa IGMP v3 - RFC 3376
10. Obsługa IGMP v1/v2/v3 snooping
11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

**Bezpieczeństwo**

1. Obsługa logowania do sieci Network Login
   1. IEEE 802.1x based Network Login
   2. MAC based Network Login
   3. Web-based Network Login
2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
7. Obsługa Guest VLAN dla IEEE 802.1x
8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
10. Obsługa TACACS+ (RFC 1492)
11. Obsługa RADIUS Authentication (RFC 2138)
12. Obsługa RADIUS Accounting (RFC 2139)
13. RADIUS per-command Authentication
14. Obsługa RADIUS over TLS (RadSec) – RFC 6614
15. Bezpieczeństwo MAC adresów
16. ograniczenie liczby MAC adresów na porcie
17. zatrzaśnięcie MAC adresu na porcie
18. możliwość wpisania statycznych MAC adresów na port/vlan
19. Możliwość wyłączenia MAC learning
20. Zabezpieczenie przełącznika przed atakami DoS
    1. Networks Ingress Filtering RFC 2267
    2. SYN Attack Protection
    3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
21. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    1. Adres MAC źródłowy i docelowy plus maska
    2. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    3. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    4. Numery portów źródłowych i docelowych TCP, UDP
    5. Zakresy portów źródłowych i docelowych TCP, UDP
    6. Identyfikator sieci VLAN - VLAN ID
    7. Quality of Service IEEE 802.1p oraz DiffServ
    8. Flagi TCP
    9. Obsługa fragmentów
22. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
23. Możliwość konfiguracji min. 8 000 reguł na wejściu i 1 000 reguł na wyjściu
24. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
25. Obsługa bezpiecznego transferu plików SCP/SFTP
26. Obsługa DHCP Option 82
27. Obsługa IP Security – Trusted DHCP Server
28. Obsługa IP Security – DHCP Snooping and Guard
29. Obsługa IP Security - Gratuitous ARP Protection
30. Obsługa IP Security – DHCP Secured ARP/ARP Validation
31. Obsługa IP Security – IP Source guard
32. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
33. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

**Bezpieczeństwo sieciowe**

1. Możliwość konfiguracji portu głównego i zapasowego
2. Obsługa redundancji routingu VRRP
3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa ERPS / G.8032
8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
10. Obsługa LACP w ramach MLAG

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP lub NTP
2. Zarządzanie przez SNMP v1/v2/v3
3. Zarządzanie przez przeglądarkę WWW – protokół http i https
4. Możliwość zarządzania przez protokół XML
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)
13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

**Inne**

1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
3. Wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
4. Obsługa skryptów CLI
5. Obsługa funkcji TCL/Tk w skryptach CLI
6. Obsługa skryptów Python
7. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
8. Możliwość rozbudowy przełącznika o „wyniesione” porty (urządzenia) zarządzane z przełącznika – przykładowo zamiast prostych niezarządzalnych 8 portowych przełączników, urządzenie zarządzalne z przełącznika nadrzędnego.
9. Możliwość uruchamiania skryptów
   1. Ręcznie
   2. O określonym czasie lub co wskazany okres czasu
   3. Na podstawie wpisów w logu systemowym
10. **Przełącznik Typ 4 – 7 szt.**
11. Przełącznik wyposażony w 48 portów 10/100/1000BASE-T
12. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
13. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
14. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
15. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
16. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
17. Wysokość urządzenia 1U montowana w standardowym 19” Rack
18. Przełącznik musi posiadać dwa zasilacze 230V, które umożliwiają uzyskanie redundancji zasilania. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
19. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
20. Porty stakujące, w przypadku niewykorzystania ich do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty SFP+ z przepustowością 10 Gb/s
21. Możliwość łączenia do 8 przełączników w stos
22. Nieblokująca architektura o wydajności przełączania min. 256 Gb/s
23. Szybkość przełączania min. 190 Milionów pakietów na sekundę
24. Temperatura pracy przełącznika w zakresie min. 0o do 50o C
25. Tablica MAC adresów min. 32 tys.
26. Pamięć operacyjna: min. 1 GB pamięci DRAM
27. Pamięć flash: min. 1 GB pamięci Flash
28. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
29. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
30. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
31. Obsługa Q-in-Q IEEE 802.1ad
32. Obsługa Quality of Service
    1. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
    2. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
    3. 8 kolejek priorytetów na każdym porcie wyjściowym
    4. Obsługa kolejek Strict Priority
    5. Obsługa kolejek Weighted Round Robin
    6. Obsługa WRED (Weighted Random Early Detection)
33. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
34. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
35. Obsługa CDPv2 z obsługą Voice VLAN
36. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
37. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
38. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
39. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
40. Możliwość monitorowania zajętości CPU oraz pamięci
41. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
42. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
43. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
44. Dedykowany port konsoli szeregowej RJ45
45. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 - forwarding
2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
   1. RIP v1/v2
   2. OSPFv2 - możliwość rozszerzenia przez licencje
   3. BGPv4 - możliwość rozszerzenia przez licencje
   4. IS-IS - możliwość rozszerzenia przez licencje
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 - forwarding
2. Pojemność tabeli routingu min. 6 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
   1. RIPng
   2. OSPF v3 – możliwość rozszerzenia przez licencje
   3. BGPv4 – możliwość rozszerzenia przez licencje
   4. IS-IS – możliwość rozszerzenia przez licencje
5. Obsługa 6to4 (RFC 3056)
6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
7. Obsłgua MLDv2 (Multicast Listener Discovery version 2)
8. Policy Based Routing dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączanie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa PIM-SM
4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
6. Obsługa Multicast VLAN Registration - MVR
7. Obsługa IGMP v1 - RFC 1112
8. Obsługa IGMP v2 - RFC 2236
9. Obsługa IGMP v3 - RFC 3376
10. Obsługa IGMP v1/v2/v3 snooping
11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

**Bezpieczeństwo**

1. Obsługa logowania do sieci Network Login
   1. IEEE 802.1x based Network Login
   2. MAC based Network Login
   3. Web-based Network Login
2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
7. Obsługa Guest VLAN dla IEEE 802.1x
8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
10. Obsługa TACACS+ (RFC 1492)
11. Obsługa RADIUS Authentication (RFC 2138)
12. Obsługa RADIUS Accounting (RFC 2139)
13. RADIUS per-command Authentication
14. Obsługa RADIUS over TLS (RadSec) – RFC 6614
15. Bezpieczeństwo MAC adresów
16. ograniczenie liczby MAC adresów na porcie
17. zatrzaśnięcie MAC adresu na porcie
18. możliwość wpisania statycznych MAC adresów na port/vlan
19. Możliwość wyłączenia MAC learning
20. Zabezpieczenie przełącznika przed atakami DoS
    1. Networks Ingress Filtering RFC 2267
    2. SYN Attack Protection
    3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
21. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    1. Adres MAC źródłowy i docelowy plus maska
    2. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    3. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    4. Numery portów źródłowych i docelowych TCP, UDP
    5. Zakresy portów źródłowych i docelowych TCP, UDP
    6. Identyfikator sieci VLAN - VLAN ID
    7. Quality of Service IEEE 802.1p oraz DiffServ
    8. Flagi TCP
    9. Obsługa fragmentów
22. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
23. Możliwość konfiguracji min. 8 000 reguł na wejściu i 1 000 reguł na wyjściu
24. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
25. Obsługa bezpiecznego transferu plików SCP/SFTP
26. Obsługa DHCP Option 82
27. Obsługa IP Security – Trusted DHCP Server
28. Obsługa IP Security – DHCP Snooping and Guard
29. Obsługa IP Security - Gratuitous ARP Protection
30. Obsługa IP Security – DHCP Secured ARP/ARP Validation
31. Obsługa IP Security – IP Source guard
32. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
33. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

**Bezpieczeństwo sieciowe**

1. Możliwość konfiguracji portu głównego i zapasowego
2. Obsługa redundancji routingu VRRP
3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa ERPS / G.8032
8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
10. Obsługa LACP w ramach MLAG

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP lub NTP
2. Zarządzanie przez SNMP v1/v2/v3
3. Zarządzanie przez przeglądarkę WWW – protokół http i https
4. Możliwość zarządzania przez protokół XML
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)
13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

**Inne**

1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
3. Wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
4. Obsługa skryptów CLI
5. Obsługa funkcji TCL/Tk w skryptach CLI
6. Obsługa skryptów Python
7. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
8. Możliwość rozbudowy przełącznika o „wyniesione” porty (urządzenia) zarządzane z przełącznika – przykładowo zamiast prostych niezarządzalnych 8 portowych przełączników, urządzenie zarządzalne z przełącznika nadrzędnego.
9. Możliwość uruchamiania skryptów
   1. Ręcznie
   2. O określonym czasie lub co wskazany okres czasu
   3. Na podstawie wpisów w logu systemowym
10. **Przełącznik Typ 5 – 8 szt.**
11. Przełącznik wyposażony w 48 portów PoE+ 10/100/1000BASE-T
12. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
13. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
14. Przełącznik musi być wyposażony w min. 4 porty SFP+ 1/10 Gb/s do połączenia przełącznika lub stosu przełączników do szkieletu sieci
15. Wszystkie porty przełącznika mają mieć możliwość wsparcia szyfracji MACsec 128/256-bit, która może być wbudowana lub zostać uruchomiona po dostarczeniu dodatkowej licencji – licencja nie jest aktualnie wymagana
16. Wszystkie porty muszą być aktywne - jeśli wymagają dodatkowych licencji zgodnie z powyższymi wymaganiami co do prędkości i liczby portów to licencje te muszą być dostarczone
17. Wysokość urządzenia 1U montowana w standardowym 19” Rack
18. Przełącznik musi posiadać dwa zasilacze 230V, które umożliwiają uzyskanie redundancji zasilania. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.
19. PoE+ zgodne ze standardem IEEE 802.3at.
20. Budżet mocy dla PoE+ min. 740W z jednego i 1480W z dwóch zasilaczy.
21. Możliwość konfiguracji priorytetów wyłączenia PoE+ w przypadku braku budżetu mocy wynikającego np. z uszkodzenia pojedynczego zasilacza.
22. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 80 Gb/s
23. Porty stakujące, w przypadku niewykorzystania ich do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty SFP+ z przepustowością 10 Gb/s
24. Możliwość łączenia do 8 przełączników w stos
25. Nieblokująca architektura o wydajności przełączania min. 256 Gb/s
26. Szybkość przełączania min. 190 Milionów pakietów na sekundę
27. Temperatura pracy przełącznika w zakresie min. 0o do 50o C
28. Tablica MAC adresów min. 32 tys.
29. Pamięć operacyjna: min. 1 GB pamięci DRAM
30. Pamięć flash: min. 1 GB pamięci Flash
31. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
32. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
33. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
34. Obsługa Q-in-Q IEEE 802.1ad
35. Obsługa Quality of Service
    1. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
    2. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
    3. 8 kolejek priorytetów na każdym porcie wyjściowym
    4. Obsługa kolejek Strict Priority
    5. Obsługa kolejek Weighted Round Robin
    6. Obsługa WRED (Weighted Random Early Detection)
36. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
37. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
38. Obsługa CDPv2 z obsługą Voice VLAN
39. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
40. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
41. Obsługa tzw. Secure Boot – kryptograficzne sprawdzanie instalowanego na przełączniku oprogramowania zapobiegające jego podmianie na oprogramowanie nieautoryzowane.
42. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
43. Możliwość monitorowania zajętości CPU oraz pamięci
44. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
45. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
46. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
47. Dedykowany port konsoli szeregowej RJ45
48. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 - forwarding
2. Pojemność sprzętowej tabeli routingu min. 12 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
   1. RIP v1/v2
   2. OSPFv2 - możliwość rozszerzenia przez licencje
   3. BGPv4 - możliwość rozszerzenia przez licencje
   4. IS-IS - możliwość rozszerzenia przez licencje
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 - forwarding
2. Pojemność tabeli routingu min. 6 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
   1. RIPng
   2. OSPF v3 – możliwość rozszerzenia przez licencje
   3. BGPv4 – możliwość rozszerzenia przez licencje
   4. IS-IS – możliwość rozszerzenia przez licencje
5. Obsługa 6to4 (RFC 3056)
6. Obsługa MLDv1 (Multicast Listener Discovery version 1)
7. Obsłgua MLDv2 (Multicast Listener Discovery version 2)
8. Policy Based Routing dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączanie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa PIM-SM
4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
6. Obsługa Multicast VLAN Registration - MVR
7. Obsługa IGMP v1 - RFC 1112
8. Obsługa IGMP v2 - RFC 2236
9. Obsługa IGMP v3 - RFC 3376
10. Obsługa IGMP v1/v2/v3 snooping
11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

**Bezpieczeństwo**

1. Obsługa logowania do sieci Network Login
   1. IEEE 802.1x based Network Login
   2. MAC based Network Login
   3. Web-based Network Login
2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
7. Obsługa Guest VLAN dla IEEE 802.1x
8. Możliwość przekierowania na Captive Portal podczas logowania do sieci
9. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
10. Obsługa TACACS+ (RFC 1492)
11. Obsługa RADIUS Authentication (RFC 2138)
12. Obsługa RADIUS Accounting (RFC 2139)
13. RADIUS per-command Authentication
14. Obsługa RADIUS over TLS (RadSec) – RFC 6614
15. Bezpieczeństwo MAC adresów
16. ograniczenie liczby MAC adresów na porcie
17. zatrzaśnięcie MAC adresu na porcie
18. możliwość wpisania statycznych MAC adresów na port/vlan
19. Możliwość wyłączenia MAC learning
20. Zabezpieczenie przełącznika przed atakami DoS
    1. Networks Ingress Filtering RFC 2267
    2. SYN Attack Protection
    3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
21. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    1. Adres MAC źródłowy i docelowy plus maska
    2. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    3. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    4. Numery portów źródłowych i docelowych TCP, UDP
    5. Zakresy portów źródłowych i docelowych TCP, UDP
    6. Identyfikator sieci VLAN - VLAN ID
    7. Quality of Service IEEE 802.1p oraz DiffServ
    8. Flagi TCP
    9. Obsługa fragmentów
22. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
23. Możliwość konfiguracji min. 8 000 reguł na wejściu i 1 000 reguł na wyjściu
24. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
25. Obsługa bezpiecznego transferu plików SCP/SFTP
26. Obsługa DHCP Option 82
27. Obsługa IP Security – Trusted DHCP Server
28. Obsługa IP Security – DHCP Snooping and Guard
29. Obsługa IP Security - Gratuitous ARP Protection
30. Obsługa IP Security – DHCP Secured ARP/ARP Validation
31. Obsługa IP Security – IP Source guard
32. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
33. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

**Bezpieczeństwo sieciowe**

1. Możliwość konfiguracji portu głównego i zapasowego
2. Obsługa redundancji routingu VRRP
3. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa ERPS / G.8032
8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
10. Obsługa LACP w ramach MLAG

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP lub NTP
2. Zarządzanie przez SNMP v1/v2/v3
3. Zarządzanie przez przeglądarkę WWW – protokół http i https
4. Możliwość zarządzania przez protokół XML
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)
13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

**Inne**

1. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
3. Wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
4. Obsługa skryptów CLI
5. Obsługa funkcji TCL/Tk w skryptach CLI
6. Obsługa skryptów Python
7. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
8. Możliwość rozbudowy przełącznika o „wyniesione” porty (urządzenia) zarządzane z przełącznika – przykładowo zamiast prostych niezarządzalnych 8 portowych przełączników, urządzenie zarządzalne z przełącznika nadrzędnego.
9. Możliwość uruchamiania skryptów
   1. Ręcznie
   2. O określonym czasie lub co wskazany okres czasu
   3. Na podstawie wpisów w logu systemowym
10. **Bezprzewodowy punkt dostępowy – 15 szt.**
11. Punkt dostępowy przeznaczony do instalacji wewnątrz pomieszczeń
12. Punkt dostępowy musi posiadać cztery interfejsy radiowe pozwalające na obsługę:
    1. Pasma 2.4 GHz min. 2x2:2 MIMO
    2. Pasma 5 GHz min. 4x4:4 MIMO
    3. Sensor min. 2x2:2 MIMO pracujący w paśmie 2.4 GHz oraz 5 GHz
    4. Bluetooth Low Energy (BLE) zgodny z IEEE 802.15.4
13. Punkt dostępowy musi zapewniać prawidłową pracę w zakresie temperatur od 00C do +500C
14. Punkt dostępowy musi być zgodny ze standardem WiFi6 – IEEE 802.11ax.
15. Punkt dostępowy musi posiadać możliwość zabezpieczenia z wykorzystaniem systemu Kensington
16. Punkt dostępowy musi być wyposażony w system montażowy pozwalający na instalację na ścianie oraz suficie (również suficie podwieszanym)
17. Punkt dostępowy musi posiadać wbudowane diody LED sygnalizujące stan pracy.
18. Punkt dostępowy musi posiadać możliwość centralnego wyłączenia diod LED sygnalizujących stan pracy oraz włączenia lokalizacji (charakterystyczna sekwencja świecenia diod LED) punktu dostępowego.
19. Punkt dostępowy musi być wyposażony w 2 interfejsy Ethernet 10/100/1000BASE-T z czego min. jeden musi zapewniać możliwość zasilenia punktu dostępowego przez PoE+ (IEEE 802.3at – max. 30W).
20. Przynajmniej jeden z powyższych interfejsów Ethernet musi wspierać Multi-rate min. 2.5 Gb/s.
21. Punkt dostępowy musi posiadać interfejs USB 3.0
22. Punkt dostępowy musi zapewniać obsługę min. 8 SSID na każdym radiu WiFi
23. Punkt dostępowy musi zapewniać możliwość dołączenia min. 500 klientów na każdym WiFi
24. Punkt dostępowy musi zapewniać możliwość pracy samodzielnej jak również pracy z wykorzystaniem dedykowanego kontrolera sieci bezprzewodowej.
25. Producent musi zapewniać dedykowane kontrolery zarówno w postaci sprzętowej jak i wirtualnej możliwej do instalacji w środowisku VMWare oraz HyperV.
26. Punkt dostępowy musi posiadać mechanizmy zapewniające współpracę z min. dwoma kontrolerami zapewniającymi odporność na awarie i możliwość dalszej pracy w przypadku uszkodzenia pojedynczego kontrolera.
27. Punkt dostępowy musi zapewniać możliwość uruchomienia w trybie kontrolera zapewaniającego możliwość zarządzania do min. 64 punktów dostępowych.
28. Punkt dostępowy musi zapewniać możliwość monitorowania i zarządzania z chmury producenta.
29. Punkt dostępowy musi posiadać możliwość konfiguracji suplikanta IEEE 802.1x i pozwalać na uwierzytelnianie z wykorzystaniem min. PEAP oraz EAP-TLS (certyfikat zainstalowany na punkcie dostępowym)
30. Punkt dostępowy musi zapewniać możliwość terminowania połączeń bezprzewodowych bezpośrednio na punkcie dostępowym i wpuszczania ruchu do wskazanej sieci VLAN (sieć VLAN musi być konfigurowalna dla każdego SSID z osobna oraz musi być możliwość jej przekazania dla każdego klienta uwierzytelnianego z wykorzystaniem systemu RADIUS w ramach RFC 3580).
31. Punkt dostępowy musi zapewniać możliwość tunelowania ruchu klienta bezprzewodowego przez sieć LAN do kontrolera i wpuszczania ruchu do wskazanej sieci VLAN na kontrolerze (sieć VLAN musi być konfigurowalna dla każdego SSID z osobna oraz musi być możliwość jej przekazania dla każdego klienta uwierzytelnianego z wykorzystaniem systemu RADIUS w ramach RFC 3580).
32. Punkt dostępowy musi zapewniać obsługę automatycznej sygnalizacji niezbędnych sieci VLAN z wykorzystaniem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB)
33. Punkt dostępowy musi zapewniać obsługę tunelowania ruchu poprzez VxLAN.
34. Ruch kontrolny oraz tunelowany pomiędzy punktem dostępowym a kontrolerem musi mieć możliwość zabezpieczenia z wykorzystaniem IPSec.
35. Punkt dostępowy musi mieć możliwość dołączenia się do kontrolera znajdującego się w innej podsieci IP np. dołączenie punktu bezprzewodowego do kontrolera znajdującego się w innej lokalizacji.
36. Punkt dostępowy musi zapewniać możliwość konfiguracji puli sieci VLAN dla obsługi dużej liczby klientów z zapewnieniem ich separacji w sieci LAN z wykorzystaniem wielu sieci VLAN.
37. Punkt dostępowy musi zapewniać realizację filtrowania ruchu dla dołączonych klientów bezprzewodowych. Filtracja musi być możliwa dla każdego SSID z osobna oraz musi być możliwość przekazania informacji o filtracji dla każdego klienta uwierzytelnionego z wykorzystaniem systemu RADIUS.
38. Filtracja ruchu musi się odbywać na punkcie bezprzewodowym.
39. Punkt dostępowy musi zapewniać realizację roamingu bez konieczności współpracy z kontrolerem.
40. Punkt dostępowy musi zapewniać wsparcie IEEE 802.11r, IEEE 802.11k oraz IEEE 802.11v
41. Punkt dostępowy musi umożliwiać współpracę z dedykowanym systemem IDS oraz IPS oferowanym przez producenta punktu dostępowego
42. Punkt dostępowy musi zapewniać możliwość uwierzytelniania klientów bezprzewodowych z wykorzystaniem IEEE 802.1x i protokołów min.: EAP-TLS, EAP-TTLS, EAP-SIM, PEAP
43. Punkt dostępowy musi zapewniać obsługę WPA3
44. Punkt dostępowy musi zapewniać możliwość uwierzytelniania klientów z wykorzystaniem MAC Authentication
45. Punkt dostępowy musi zapewniać współpracę z serwerami RADIUS Authentication oraz RADIUS Accounting
46. Punkt dostępowy musi zapewniać możliwość uwierzytelniania z wykorzystaniem Microsoft Active Directory
47. Punkt dostępowy musi zapewniać realizację priorytetów dla rozwiązań VoIP z wykorzystaniem: IEEE 802.11e/WMM, U-APSD, TSPEC, CAC, QBSS
48. Punkt dostępowy musi zapewniać wsparcie zabezpieczenia ramek kontrolnych zgodnie ze standardem IEEE 802.11w
49. Punkt dostępowy musi zapewniać obsługę gości poprzez Captive Portal uruchomiony na punkcie dostępowym lub kontrolerze lub na zewnętrznym systemie kontroli dostępu.
50. Punkt dostępowy musi zapewniać możliwość przekierowania klientów bezprzewodowych na Captive Portal
51. Punkty dostępowe muszą zapewniać automatyczne wykrywanie najmniej zakłóconych kanałów oraz dostosowywać moc promieniowania dla zapewnienia jak najmniejszych zakłóceń z innymi punktami pracującymi na tym samym kanale przy zapewnienie optymalnego zasięgu.
52. Punkty dostępowe musza zapewniać zapewnienie równego dostępu wszystkich obsługiwanych urządzeń do sieci bezprzewodowej tzw. airtime fairness
53. Punkt dostępowy musi zapewniać możliwość separacji ruchu typu Bonjour and UPNP do wydzielonej sieci VLAN
54. Punkt dostępowy musi zapewniać możliwość filtracji oraz ograniczania ruch dla aplikacji (bazując na warstwie 7 modelu OSI) z możliwością wyboru pojedynczych lub grup aplikacji – np. filtracja aplikacji streamingowych typu: YouTube, Netflix, HBO GO, Apple iTunes itp., filtracja aplikacji peer to peer typu: BitTorrent, Kazaa, Gnutella itp., filtracja aplikacji Cloud Storage typu: Google Drive, Dropbox, Box, iCloud, iPhoto itp.
55. Punkt dostępowy musi posiadać Certyfikat CE lub Deklarację zgodności
56. Punkt dostępowy musi posiadać tzw. dożywotnią gwarancję, czyli zapewnienie wymiany w przypadku awarii do min. 5 lat po zakończeniu produkcji urządzenia.
57. **Kontroler punktów bezprzewodowych**
58. Kontroler bezprzewodowy instalowany jako maszyn wirtualna
59. Kontroler bezprzewodowy musi wspierać instalację w systemie VMWare oraz HyperV
60. Kontroler musi zapewniać możliwość skalowania liczby obsługiwanych punktów dostępowych oraz klientów bezprzewodowych poprzez zmianę udostępnianych zasobów w środowisku wirtualnym
61. Kontroler musi zapewniać możliwość pracy w klastrze odpornym na awarie
62. Kontroler musi zapewniać skalowalność do min. 1000 punktów dostępowych i 16 tys. klientów bezprzewodowych
63. Kontroler musi zapewniać obsługę sieci VLAN zgodnych z IEEE 802.1Q
64. Kontroler musi być zarządzany przez przeglądarkę www bez konieczności instalacji aplikacji na stacji zarządzającej jak np. Java
65. Kontroler musi zapewniać obsługę wielu Lokalizacji z wizualizacją ich stanu, liczby sieci bezprzewodowych (SSID) oraz liczby obsługiwanych punktów dostępowych w każdej lokalizacji.
66. Kontroler musi posiadać integrację z systemem map pozwalających na wizualizację poszczególnych lokalizacji na mapie i określeniem lokalizacji poprzez jej wskazanie na mapie lub wpisanie współrzędnych geograficznych
67. Kontroler musi zapewniać możliwość konfiguracji planów poszczególnych pięter budynków oraz umieszczenie punktów dostępowych na planie
68. Kontroler musi zapewniać możliwość nanoszenia na plany budynków ścian i pozwalać na wizualizację zasięgu poszczególnych punktów dostępowych umieszczonych na planie.
69. Kontroler musi zapewniać możliwość importu planów z systemu planowania Ekahau (ESX) jak również wczytywanie planów piętra z plików graficznych
70. Kontroler musi zapewniać widzialność wszystkich dołączonych do kontrolera punktów dostępowych z następującymi informacjami:
    1. Nazwa punktu dostępowego – konfigurowalna nazwa punktu (Host Name)
    2. Typ punktu dostępowego
    3. Numer seryjny punktu dostępowego
    4. MAC adres punktu dostępowego
    5. Adres IP punktu dostępowego
    6. Status punktu dostępowego
    7. Przypisanie do lokalizacji
    8. Informacje o kanałach pracy poszczególnych interfejsów radiowych
    9. Informacje o liczbie klientów na poszczególnych interfejsach radiowych
    10. Informacje o aktualnej mocy ustawionej na poszczególnych interfejsach radiowych
    11. Informacji o szerokości kanału ustawionej na poszczególnych interfejsach radiowych
    12. Informacji o statusie portów Ethernet i ewentualnej konfiguracji połączeń Link Aggregation na portach Etherent punktów dostępwowych
    13. Informacji o poziomie szumu dla poszczególnych interfejsów radiowych
71. Kontroler musi zapewniać możliwość filtracji prezentowanych informacji o punktach dostępowych na podstawie dowolnych parametrów z uwzględnieniem warunków logicznych np. wszystkie punkty w lokalizacji Warszawa pracujące na kanale 36
72. Kontroler musi zapewniać możliwość konfiguracji sieci bezprzewodowych, ich przydziału do grup punktów dostępowych, a następnie do lokalizacji
73. Kontroler musi zapewniać automatyczne wykrywanie nowych punktów dostępowych
74. Kontroler musi być zarządzany przez SNMPv1/v2/v3 oraz SSHv2.
75. Kontroler musi obsługiwać RADIUS authentication oraz RADIUS accounting.
76. Kontroler musi zapewniać obsługę: 802.11i, WPA, WPA2, TKIP oraz AES, WPA3
77. Kontroler musi zapewniać obsługę IEEE 802.1x oraz autentykację: EAP-TLS, EAP-TTLS, PEAP oraz EAP-SIM.
78. Kontroler musi zapewniać obsługę uwierzytelniania MAC authentication
79. Kontroler musi zapewniać przesyłanie danych z sieci WLAN do sieci przewodowej w następujących architekturach:
    1. bridging na kontrolerze – kontroler zapewnia przełączanie ruchu z sieci bezprzewodowej do wskazanej sieci wirtualnej przewodowej dołączonej do kontrolera
    2. bridging na punkcie dostępowym – w tym trybie ruch z sieci bezprzewodowej jest kierowany bezpośrednio do wskazanej sieci wirtualnej przyłączonej bezpośrednio do punktu dostępowego
    3. bridging na punkcie dostępowym wraz z sygnalizacją niezbędnych sieci VLAN z wykorzystaniem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB)
    4. bridging na punkcie dostępowym z zapewnieniem tunelowania ruchu poprzez VxLAN
80. Kontroler bezprzewodowy musi zapewniać możliwość ustawiania następujących parametrów w ramach każdej sesji klienckiej:
    1. indywidualne raguły filtrowania ruchu
    2. przypisanie sieci VLAN
    3. QoS
    4. ograniczenia transmisji wejściowej i wyjściowej
    5. wyboru topologii (bridging na kontrolerze, bridging na punkcie dostępowym, tunel VxLAN, IEEE 802.1Qcj)
81. Kontroler musi zapewniać obsługę Captive Portal pozwalającego na obsługę gości jak i uwierzytelnianie klientów bezprzewodowych z wykorzystaniem Captive Portal – np. nie posiadających suplikanta IEEE 802.1x
82. Kontroler musi zapewniać możliwość rejestracji gości w oparciu o portal www znajdujący się na kontrolerze.
83. Portal rejestracji gości musi zapewniać możliwość konfiguracji danych niezbędnych dla rejestracji np.: Imię, Nazwisko, email, numer telefonu, PESEL, nr. Dowodu itp.
84. Portal rejestracji gości musi zapewniać możliwość stworzenia i akceptacji regulaminu przez rejestrujących się gości
85. Kontroler musi zapewniać przynajmniej podstawową konfigurację wyglądu Captive Portal – zmiana kolorów, zmiana stylów CSS, dodanie loga firmy
86. Captive Portal musi posiadać możliwość obsługi wielu języków wybieranych automatycznie na podstawie ustawień przeglądarki klienta bezprzewodowego jak również za pomocą np. combo box na portalu.
87. Captive Portal musi zapewniać wsparcie min. języka polskiego, angielskiego i niemieckiego.
88. Captive Portal musi zapewniać obsługę urządzeń mobilnych
89. Kontroler musi zapewniać rejestrację gości z wykorzystaniem portali społecznościowych np. Facebook, Google, Yahoo
90. Kontroler musi zapewniać możliwość automatycznej, centralnej aktualizacji oprogramowania punktów dostępowych zaadoptowanych do kontrolera.
91. Kontroler musi zapewniać możliwość konfiguracji blokowania ruchu pomiędzy klientami sieci bezprzewodowej.
92. Kontroler musi zapewniać autoryzację użytkowników IEEE 802.1x w oparciu o zewnętrzny serwer RADIUS z możliwością definicji różnych serwerów RADIUS dla różnych identyfikatorów SSID
93. Kontroler musi zapewniać przydzielanie klientów do wskazanych sieci wirtualnych na podstawie informacji przesyłanej z serwera RADIUS zgodnie z RFC3580
94. Kontroler musi zapewniać możliwość uwierzytelniania z wykorzystaniem Microsoft Active Directory
95. Kontroler musi zapewniać możliwość przydzielania do sieci VLAN na podstawie przynależności klientów bezprzewodowych do grup użytkowników zdefiniowanych w LDAP
96. Kontroler musi zapewniać przydzielanie polityki zawierającej QoS (Quality of Service), list kontroli dostępu ACL. Przydzielane polityki muszą być realizowane na punktach dostępowych w przypadku ruchu, który jest wpuszczany do sieci bezpośrednio na punkcie dostępowym.
97. Kontroler musi zapewniać konfigurację roamingu pomiędzy punktami dostępowymi.
98. Kontroler musi zapewniać konfigurację oszczędzania energii UAPSD (Unscheduled Automatic Power Save Delivery).
99. Kontroler musi obsługiwać QBSS (informacja o zbyt dużym obciążeniu zostanie przekazana klientowi dla obsługi inteligentnego roamingu)
100. Kontroler musi obsługiwać funkcjonalność FCA (Flexible Client Access) zwiększającą prędkość transmisji klientów IEEE 802.11n w sieci z urządzeniami IEEE 802.11/a/b/g.
101. Kontroler musi obsługiwać funkcjonalność CAC (Call Admission Control), pozwalającą na sprawdzenie, czy zestawienie nowego połączenia telefonii VoIP nie wpłynie na jakość dotychczasowych połączeń.
102. Kontroler musi zapewniać obsługę preferencji pasma polegającą na automatycznym przenoszeniu klientów na pasmo 5 GHz.
103. Kontroler musi zapewniać możliwość uruchamianie sieci bezprzewodowych wg. skonfigurowanego planu bazującego na kalendarzu.
104. Kontroler musi obsługiwać wszystkie dostarczone punkty bezprzewodowe (musi zostać dostarczony z licencją na obsługę min. 15 punktów dostępowych)
105. **Oprogramowanie zarządzające wraz z systemem NAC**

* Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
  + Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
  + Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
* Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
* Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami oraz wszystkimi dostarczonymi punktami dostępowymi.
* Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
* Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
* Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
* Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
* Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
* Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
* Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
* Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
* Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
* Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email’a, wysłanie trapu SNMP, wpisu do Syslog’a lub uruchomienie skryptu.
* Aplikacja musi posiadać wbudowany Syslog serwer.
* Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
* Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
* Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.
* Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
  + Wysłanie e-mail do wskazanej grupy adresowej
  + Wysłanie informacji SYSLOG do wskazanego serwera
  + Wysłanie TRAP SNMP do wskazanego adresu IP
  + Uruchomienie skryptu w systemie operacyjnym Linux
  + Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
* Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
* Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
* Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
* Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
  + połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
  + konfiguracji sieci VLAN
* Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
* Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
  + adres IP urządzenia
  + adresu MAC urządzenia
  + nazwy urządzenia
  + wersji oprogramowania
  + wersji bootrom
  + lokalizacji urządzenia
  + danych kontaktowych administratora
  + numeru seryjnego
  + numeru inwentaryzacyjnego – własna numeracja
* Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
  + możliwość automatycznej periodycznej realizacji backup’u konfiguracji urządzeń o wskazanym czasie
  + możliwość realizacji backup’u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
  + możliwość odtworzenia wskazanej konfiguracji urządzenia
  + możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
  + możliwość obsługi backup’u urządzeń sieciowych różnych producentów
* Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
* Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
* Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
* Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
* Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
  + przyłączenia do sieci VLAN
  + przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,
  + konfiguracji Quality of Service
  + konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
  + możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.
* Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
  + szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
  + wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
  + wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
  + generowanie raportów
* Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
  + Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
  + Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
  + Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
    - adres IP kontrolera
    - liczba obsługiwanych klientów
    - szczytowe wartości zajmowanego pasma
    - wersja oprogramowania
  + Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
    - adres IP punktu dostępowego
    - MAC adres punktu dostępowego
    - wersja oprogramowania
    - typ punktu dostępowego
    - kanały pracy poszczególnych interfejsów radiowych
    - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
  + Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
    - adres IP klienta
    - MAC adres klienta
    - nazwa użytkownika
    - nazwa punktu dostępowego, do którego dołączony jest użytkownik
    - BSSID, do którego dołączony jest użytkownik
    - SSID, do którego dołączony jest użytkownik
  + Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
    - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
    - zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
    - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
* Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
  + adresu MAC
  + adresu IP
  + nazwy komputera
  + typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
  + nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
  + adres IP urządzenia, do którego dołączony jest klient.
  + identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
  + typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
  + nazwa przydzielonej polityki bezpieczeństwa.
* System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
* System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
* System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
  + Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
  + Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
  + Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
  + Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
  + Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
* System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
* Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
* System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
* System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS
* System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
* System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.
* System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
* System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
  + liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
  + liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
  + liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
  + liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
  + liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
* System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
* System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 500urządzeń klienckich (adresów MAC).
* System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
* System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
* System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
* System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
* System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
* System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:
  + Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
  + Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM
* System zarządzania musi być objęty **3 letnim** wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.

1. **Inne**
   1. Wszystkie urządzenia muszą zostać dostarczone z minimum 3 letnim wsparciem technicznym producenta obejmującym co najmniej: wymianę uszkodzonego urządzenia w trybie NBD AHR, dostęp do aktualizacji oprogramowania, dostęp do wsparcia technicznego producenta, dostęp do bazy wiedzy technicznej
   2. Kontroler sieci bezprzewodowej musi zostać dostarczony z minimum 3 letnim wsparciem technicznym producenta obejmującym co najmniej: dostęp do aktualizacji oprogramowania, dostęp do wsparcia technicznego producenta, dostęp do bazy wiedzy technicznej
   3. Oprogramowanie zarządzające musi zostać dostarczone w wersji on-premise lub subskrybcji z zapewnionym minimum 3 letnim wsparciem technicznym producenta obejmującym co najmniej: dostęp do aktualizacji oprogramowania, dostęp do wsparcia technicznego producenta, dostęp do bazy wiedzy technicznej
   4. Wraz z przełącznikami należy dostarczyć moduły światłowodowe i kable DAC w następujących ilościach:
      1. 50 szt. modułów światłowodowych SFP+ 10GBase-LR
      2. 60 szt. modułów światłowodowych SFP+ 10GBase-SR
      3. 4 szt. modłów światłowodowych SFP 1GBase-SX
      4. 4 szt. kabli DAC QSFP28 100G dł. 1m
   5. Wszystkie urządzenia oraz oprogramowanie do zarządzania oferowane w tym postępowaniu muszą być ze sobą kompatybilne i umożliwiać wdrożenie standardu IEEE 802.1X wraz z posiadanymi przez Zamawiającego przełącznikami Extreme Networks x620-16x
   6. Oferowane przełączniki Typ 2, 3, 4, 5 muszą umożliwiać zastawienie połączeń ringowych zgodnych z RFC 3619 i G.8032 z posiadanymi przez Zamawiającego przełącznikami Extreme Networks x620-16x
   7. Przełącznik Typ 1 musi umożliwiać zestawienie połączeń zgodnie ze standardem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging z posiadanymi przez Zamawiającego przełącznikami Extreme Networks x620-16x
   8. Wykonawca udziela zamawiającemu 3 letniej gwarancji na prawidłowe funkcjonowanie urządzeń w zakresie pkt. IX .5 – 7. W wypadku zaistnienia problemów w tym okresie związanych z funkcjonowaniem urządzeń zgodnie z pkt. IX .5 – 7 stosuje się par. 1 pkt 5-9 umowy.

**Część II**

**Monitor komputerowy – szt. 1**

|  |  |
| --- | --- |
| **Nazwa parametru** | **Wymagane minimalne parametry techniczne** |
| Przekątna | 34 cale |
| Rozdzielczość | 3440 x 1440 (WQHD) |
| Format obrazu | 21:9 |
| Typ | VA |
| Kontrast | 3500:1 (statyczny) |
| Jasność | 250 cd/m² |
| Czas reakcji | Maksymalnie 5 ms (gray to gray) |
| Kąt widzenia | 178° (w pionie)  178° (w poziomie) |
| Wielkość plamki | Maksymalnie 0,231 mm |
| Zużycie energii | Maksymalnie 50 W (normalna praca) |
| Porty i złącza | 1 x DisplayPort 1.2  1 x HDMI 2.0  1 x USB typ C  4 x USB 3.2 typ A |
| Funkcje | Możliwość montażu na ścianie  Regulacja wysokości i nachylenia  Tryb niskiej emisji niebieskiego światła  Eliminacja migotania obrazu |
| Dodatkowe wyposażenie | 1 x kabel zasilający  1 x kabel HDMI  1 x kabel DisplayPort  1 x kabel USB typu C |
| Zgodność z normami / Certyfikaty | ENERGY STAR  CE  ISO 9241-307  TCO Certified  - lub równoważne |
| Gwarancja | Czas: 36 miesięcy |

**Część III**

**Laptop – szt.10**

|  |  |
| --- | --- |
| **Nazwa parametru/podzespołu** | **Wymagane minimalne parametry techniczne** |
| Typ | Komputer przenośny typu notebook |
| Zastosowanie | Komputer będzie wykorzystywany do pracy naukowo-badawczej, do obsługi standardowych aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu, poczty elektronicznej oraz jako lokalna baza danych. |
| Procesor | Ilość rdzeni: 4  Zaproponowany procesor musi uzyskać w teście Passmark CPU Mark łącznie  wynik: minimum 10 000 punktów (według wyników opublikowanych na stronie [http://www.cpubenchmark.net/cpu\_list.php,](http://www.cpubenchmark.net/cpu_list.php) wg rankingu z dnia 19.09.2021 r. lub posiadać równoważne parametry i funkcjonalność, które wykonawca wykaże w równoważny sposób. |
| Pamięć operacyjna | Pojemność: 8 GB  Rodzaj: DDR4  Wolna ilość gniazd: 1 |
| Płyta główna | Musi umożliwiać pracę procesora z maksymalną wydajnością |
| Dysk twardy | Typ: SSD  Pojemność: 256 GB  Typ interfejsu: M.2 PCIe  Możliwość montażu dysku SATA |
| Karta graficzna | Kompatybilna z DirectX 12, OpenGL 4.5  Zaproponowana karta graficzna musi uzyskać w teście Passmark – G3D Mark wynik co najmniej 2800 punktów według wyników kart graficznych publikowanych na stronie <http://www.videocardbenchmark.net/gpu_list.php,> wg rankingu z dnia 19.09.2021 r. lub posiadać równoważne parametry i funkcjonalność, które wykonawca wykaże w równoważny sposób. |
| Karta dźwiękowa | Typ: zintegrowana  Wbudowane 2 głośniki |
| Komunikacja | LAN 10/100/1000 Mbps Ethernet RJ 45 zintegrowana z płytą główną  Wi-Fi 802.11ac  Moduł Bluetooth |
| Ekran | Przekątna ekranu: 15,6 cali  Rozdzielczość ekranu: 1920 x 1080 pikseli (Full HD) |
| Porty i złącza | 2 x USB 3.2 Gen 1 Type-A  1 x USB 2.0 Type-A  1 x RJ-45  1 x HDMI 1.4  1 x Czytnik kart pamięci  1 x wyjście słuchawkowe/wejście mikrofonowe |
| Bateria i zasilacz | Pojemność baterii: 40 Wh  Zasilacz dedykowany do oferowanego laptopa |
| Kamera | Typ: zintegrowana |
| Klawiatura | Układ: QWERTY  Wydzielona klawiatura numeryczna |
| Waga | Maksymalnie 2 kg (z baterią) |
| Bezpieczeństwo | Moduł TPM |
| Dodatkowe wyposażenie | Mysz komputerowa: przewodowa |
| Zainstalowany system operacyjny | Fabrycznie nowy, nieużywany i nieaktywowany nigdy wcześniej na innym  urządzeniu system operacyjny Microsoft Windows 10 Professional (wersja 64- bitowa) lub równoważny, kompatybilny ze sprzętem i dołączonymi sterownikami, system w polskiej wersji językowej wraz z licencją nieograniczoną w czasie. Parametry spełniające warunki równoważności:   1. Pełna integracja z domeną Active Directory posiadaną przez Zamawiającego. 2. Zarządzanie poprzez Zasady Grupy (GPO) Active Directory posiadaną przez Zamawiającego. 3. Współpraca z procesorami o architekturze x86-64. 4. Możliwość wykonywania kopii zapasowej i przywracania do i z zasobów sieciowych. 5. Dostępność aktualizacji i poprawek do systemu operacyjnego u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek. 6. Możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Office 2016. 7. Możliwość udostępniania i przejmowania pulpitu zdalnego.   Wykonawca oferując równoważny system operacyjny zobowiązany jest wykazać jego równoważność do wyżej wymienionych kryteriów oraz dokonać przeszkolenia użytkowników w wymiarze 10 godzin w siedzibie Zamawiającego. |
| Gwarancja | Czas: 36 miesięcy  Naprawa w miejscu użytkowania (on-site)  Czas reakcji serwisu: maksymalnie w następnym dniu roboczym  Gwarancja obejmuje wszystkie elementy oferowanego komputera  W przypadku awarii dysków twardych, wymiana na nowe. Dyski uszkodzone pozostają własnością Zamawiającego |

**Część IV**

Przedmiotem postępowania jest zakup usługi zapewnienia wsparcia producenta oprogramowania VMWare na okres do dn. 13-10-2023 r. dla posiadanego przez Zamawiającego oprogramowania objętego kontraktem nr 494690804.

Wsparcie musi obejmować m.in.:

* wsparcie techniczne pozwalające na dostęp do pomocy technicznej producenta w trybie 8x5 NBD
* dostęp do aktualizacji oprogramowania

**Załącznik nr 4 – Formularz ofertowy**

(wypełnia wykonawca )

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia, zgodny z SWZ w tym zwłaszcza zał. Nr 3 do SWZ

**Część I**

Zakup i dostawa przełączników sieciowych, bezprzewodowych punktów dostępowych, kontrolera punktów bezprzewodowych, oprogramowania zarządzającego wraz z systemem NAC

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) –  podać dla **każdego** opisanego w SWZ przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Jednocześnie oferuję dodatkowo następujące funkcjonalności/parametry przedmiotu zamówienia ( właściwe zaznaczyć – uwaga deklarując TAK wykonawca musi spełnić wszystkie elementy opisu wyszczególnione pod danym punktem I,II lub III – zamawiający nie punktuje jedynie częściowego spełnienia któregokolwiek z opisanych w pkt I, II i III wymagań ):**

**I.** **dodatkowa funkcja analityki (D)**

tj. oprogramowanie do zarządzania zapewnia realizację funkcji analityki obejmującą co najmniej:  
• System zarządzania musi posiadać przy współpracy z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej  
• Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.  
• Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.  
• System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos  
• System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.  
• Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.  
• System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.  
• System Analityki musi zapewniać możliwość tworzenia raportów.  
• System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.

**□ -** TAK

**□ -**NIE   
  
**II. obsługa więcej niż 1000 urządzeń klienckich (adresów MAC) – (E)**

**oprogramowanie musi zostać dostarczone z odpowiednimi licencjami**

**□ -**TAK

**□ -**NIE   
  
**III. integracja z systemami innych producentów oprogramowania do zarządzania – (F)**• System zarządzania posiada wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów: Palo Alto, Fortinet, Checkpoint

• Możliwość integracji systemu kontroli tożsamości z systemami firewall co najmniej z następującymi producentami: Palo Alto, Fortinet, Checkpoint

**□ -**TAK

□ -NIE

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

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).

**Część II**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia, zgodny z SWZ w tym zwłaszcza zał. Nr 3 do SWZ

**Monitor komputerowy – szt. 1**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – dla każdego z ww. przedmiotów zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

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).

**Część III**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia, zgodny z SWZ w tym zwłaszcza zał. Nr 3 do SWZ

**Laptop – szt.10**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

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).

**Część IV**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia, zgodny z SWZ w tym zwłaszcza zał. Nr 3 do SWZ

**Zakup usługi zapewnienia wsparcia producenta dla oprogramowania VMWare posiadanego przez Zamawiającego**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

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).

1. Uczestnictwo w szkoleniu jest bezpłatne, nie wlicza się również w czas i zakres świadczenia usługi dla Instytutu [↑](#footnote-ref-1)