|  |  |
| --- | --- |
| **DZIAŁ ZAMÓWIEŃ PUBLICZNYCH** **UNIWERSYTETU JAGIELLOŃSKIEGO**ul. Straszewskiego 25/3 i 4, 31-113 Kraków**tel. +4812-663-39-03,** **e-mail: bzp@uj.edu.pl** [**www.uj.edu.pl**](http://www.uj.edu.pl) **www.przetargi,uj.edu.pl**  |  |

Kraków, dnia 16 grudnia 2021 r.

**SPECYFIKACJA WARUNKÓW ZAMÓWIENIA**

**zwana dalej w skrócie SWZ**

**Rozdział I – Nazwa (firma) oraz adres zamawiającego**

1. Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków.
2. Jednostka prowadząca sprawę:
	1. Dział Zamówień Publicznych, ul. Straszewskiego 25/3 i 4, 31-113 Kraków;

tel.: +4812 663-39-03; e-mail.: bzp@uj.edu.pl ; piotr.molczyk@uj.edu.pl

godziny urzędowania: poniedziałek-piątek; 7:30 do 15:30; z wyłączeniem dni ustawowo wolnych od pracy;

* 1. strona internetowa: [www.przetargi.uj.edu.pl](http://www.przetargi.uj.edu.pl);
	2. adres strony internetowej prowadzonego postępowania, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem: [https://przetargi.uj.edu.pl/](https://przetargi.uj.edu.pl/ogloszenia-o-postepowaniach)

**Rozdział II – Tryb udzielenia zamówienia**

1. Postępowanie prowadzone jest w **trybie przetargu nieograniczonego**, na podstawie art. 132 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j.: Dz.U. z 2019 r., poz. 2019 z późn zm.; tj. Dz.U. z 2021 r., poz. 1129 z późn. zm.), zwanej dalej „ustawą PZP”, oraz zgodnie z wymogami określonymi w niniejszej SWZ.
2. Do czynności podejmowanych przez zamawiającego i wykonawców w postępowaniu o udzielenie przedmiotowego zamówienia stosuje się przepisy powołanej ustawy PZP oraz wydanych na jej podstawie aktów wykonawczych, a w sprawach nieuregulowanych przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2020 r., poz. 1740 z późn. zm.).
3. Postępowanie prowadzone jest przez komisję przetargową powołaną do przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.

**Rozdział III – Opis przedmiotu zamówienia**

* 1. Przedmiotem postępowania i zamówienia jest wyłonienie Wykonawcy w zakresie dostawy sprzętu komputerowego oraz oprogramowania wraz z montażem w ramach modernizacji infrastruktury sieciowej przewodowej oraz bezprzewodowej w budynku Wydziału Biochemii, Biofizyki i Biotechnologii Uniwersytetu Jagiellońskiego.
	2. Oznaczenie przedmiotu zamówienia według kodu Wspólnego Słownika Zamówień CPV:

Główny kod CPV: 30200000-1 - Urządzenia komputerowe

31214100-0 - Przełączniki

32413100-2 - Rutery sieciowe

32420000-3 - Urządzenia sieciowe

32421000-0 - Okablowanie sieciowe

32562000-0 - Kable światłowodowe

48000000-8 - Pakiety oprogramowania i systemy informatyczne

48820000-2 - Serwery

72268000-1 - Usługi dostawy oprogramowania

72260000-5 - Usługi w zakresie oprogramowania

72267000-4 - Usługi w zakresie konserwacji i napraw oprogramowania

51610000-1 - Usługi instalowania urządzeń komputerowych i przetwarzania informacji

80510000-2 - Usługi szkolenia specjalistycznego

* 1. Warunki realizacji zamówienia zawarte zostały we wzorze umowy stanowiącym integralną część SWZ.
	2. ***Ogólne warunki udziału w postępowaniu:***

4.1 wykonawca musi zaoferować przedmiot zamówienia zgodny z wymogami zamawiającego, określonymi w niniejszej SWZ;

* 1. Szczegółowy opis przedmiotu zamówienia zawiera Załącznik A do SWZ.
	2. Wykonawca oświadcza, że znana jest mu sytuacja społeczno-gospodarcza zaistniała w dniu złożenia oferty w postępowaniu o udzielenie niniejszego zamówienia publicznego oraz w dniu zawarcia niniejszej Umowy, a ewentualne ryzyko związane z niedostępnością zaoferowanego modelu sprzętu komputerowego lub koniecznością zaoferowania modelu o nie gorszych parametrach technicznych niż w modelu objętym umową wkalkulował w cenę oferty, w tym cenę jednostkową oferowanego sprzętu komputerowego.

**Rozdział IV – Przedmiotowe środki dowodowe (składane wraz z ofertą)**

1. Zamawiający wymaga złożenia wraz z ofertą przedmiotowych środków dowodowych odpowiednio do każdej z części zamówienia:

1.1 opisu/ów technicznego/ych sporządzonych przez producenta i/lub wydruk/i ze stron internetowych producenta, bądź katalog/ katalogi producenta/ów, pozwalające na ocenę zgodności oferowanych urządzeń oraz ich parametrów z wymaganiami SWZ. Wykonawca musi jednoznacznie wskazać, której pozycji dotyczą przedkładane materiały. Zamawiający dopuszcza złożenie wskazanych powyżej przedmiotowych środków dowodowych w języku angielskim.

1. W przypadku, gdy zaproponowane przez wykonawcę rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia, wykonawca musi udowodnić w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że oferowane dostawy spełniają określone przez zamawiającego wymagania, cechy lub kryteria.
2. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wzywa do ich złożenia lub uzupełnienia w wyznaczonym terminie, nie krótszym niż dwa (2) dni robocze.
3. Przepisu ust. 3 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
4. Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowychZamawiający nie wymaga złożenia wraz z ofertą przedmiotowych środków dowodowych.

**Rozdział V – Termin wykonania zamówienia**

1. Przedmiot zamówienia musi zostać wykonany w terminie 12 miesięcy, licząc od dnia udzielenia zamówienia tj. od zawarcia umowy.
2. Wykonawca zapewnia gotowość do realizacji zamówienia w dniu zawarcia umowy.
3. Zamawiający dopuszcza wcześniejszą realizację zamówienia.
4. Zamawiający informuje wszystkich zainteresowanych Wykonawców o możliwości dokonania **wizji lokalnej miejsca objętego zakresem zamówienia**, po wcześniejszym uzgodnieniu terminu. Osoba do kontaktów: Pan Wojciech Pilch, tel.: 506 006 069. Zamawiający informuje, iż do złożenia oferty nie jest wymagane przeprowadzenie wizji lokalnej, a jedynie zalecane.

**Rozdział VI – Opis warunków podmiotowych udziału w postępowaniu**

1. Zdolność do występowania w obrocie gospodarczym – zamawiający nie wyznacza warunku w tym zakresie;
2. Uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów – zamawiający nie wyznacza warunku w tym zakresie;
3. Sytuacja ekonomiczna lub finansowa – zamawiający nie wyznacza warunku w tym zakresie;
4. Zdolność techniczna lub zawodowa –
	1. o udzielenie zamówienia ubiegać się może wykonawca, który spełnia warunek dotyczący zdolności zawodowej, a w szczególności wykaże, iż w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał, a w przypadku świadczeń okresowych lub ciągłych również wykonuje co najmniej dwa zamówienia (dwa odrębne kontrakty) związane z wykonaniem lub modernizacją sieci, o wartości min. 500.000,00 zł brutto każda, a kontrakty te zostały wykonane lub są wykonywane należycie. Dodatkowo, celem potwierdzenia spełnienia ww. warunku udziału w postępowaniu, zamawiający wymaga wskazania dokładnej nazwy zrealizowanego zamówienia, pozwalającej na jednoznaczną i niebudzącą wątpliwości identyfikację, wraz ze szczegółowym podaniem jego zakresu. Do przeliczenia na PLN wartości wskazanej w dokumentach złożonych na potwierdzenie spełniania warunków udziału w postępowaniu, wyrażonej w walutach innych niż PLN, zamawiający przyjmie średni kurs publikowany przez Narodowy Bank Polski dla tej waluty z dnia publikacji ogłoszenia o zamówieniu.
5. **Weryfikacji i oceny warunków udziału w postępowaniu zamawiający dokona na podstawie oświadczeń i dokumentów składanych przez uczestniczących w postępowaniu wykonawców z zachowaniem sposobu i formy, o których mowa w niniejszej SWZ**.
6. Wykonawca może w celu potwierdzenia spełniania warunków udziału, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
7. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.
8. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
	1. Warunek dotyczący uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, jest spełniony, jeżeli co najmniej jeden z wykonawców wspólnie ubiegających się o udzielenie zamówienia posiada uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej i zrealizuje dostawy, do których realizacji te uprawnienia są wymagane.
	2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Powyższe zobowiązanie lub inny środek dowodowy składa się w formie, o której mowa w rozdziale IX ust. 1.6.3-1.6.4 niniejszej SWZ.
9. Oceniając zdolność techniczną lub zawodową, zamawiający może, na każdym etapie postępowania, uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.

**Rozdział VII – Podstawy wykluczenia wykonawców**

1. Zamawiający wykluczy wykonawcę w przypadku zaistnienia okoliczności przewidzianych postanowieniami art. 108 ust. 1 PZP, z zastrzeżeniem art. 110 ust. 2.
2. Stosownie do treści art. 109 ust. 1 ustawy PZP, zamawiający wykluczy z postępowania wykonawcę:
	1. który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, 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 ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności (art. 109 ust. 1 pkt 1);
	2. w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury (art. 109 ust.1 pkt 4);
	3. który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów (art. 109 ust. 1 pkt 5);
	4. który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady (art. 109 ust. 1 pkt 7);
	5. który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych (art. 109 ust. 1 pkt 8);
	6. który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia (art. 109 ust. 1 pkt 9);
	7. który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia (art. 109 ust. 1 pkt 10).
3. W przypadkach, o których mowa w ust. 2.1 – 2.4 niniejszego rozdziału, zamawiający może nie wykluczać wykonawcy, jeżeli wykluczenie byłoby w sposób oczywisty nieproporcjonalne, w szczególności, gdy kwota zaległych podatków lub składek na ubezpieczenie społeczne jest niewielka albo sytuacja ekonomiczna lub finansowa wykonawcy, o którym mowa w ust. 2.2 powyżej, jest wystarczająca do wykonania zamówienia.

**Rozdział VIII – Wykaz oświadczeń i dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu oraz braku podstaw do wykluczenia**

1. Oświadczenia składane obligatoryjnie wraz z ofertą:
	1. w celu potwierdzenia spełnienia warunków udziału w postępowaniu oraz braku podstaw do wykluczenia, o których mowa w rozdziale VII niniejszej SWZ, wykonawca musi dołączyć do oferty jednolity dokument (JEDZ), którego wzór stanowi załącznik nr 1 do formularza ofertowego. Celem uzupełnienia oświadczenia w formie JEDZ należy go pobrać, ze strony [www.przetargi.uj.edu.pl](http://www.przetargi.uj.edu.pl), zapisać na dysku, a następnie zaimportować i uzupełnić poprzez serwis ESPD dostępny pod adresem: http://espd.uzp.gov.pl Uzupełniony ESPD należy podpisać podpisem kwalifikowanym. Serwis ESPD nie archiwizuje plików.

Zamawiający informuje, iż na stronie Urzędu Zamówień Publicznych:

<https://www.uzp.gov.pl/baza-wiedzy/prawo-zamowien-publicznych-regulacje/prawo-krajowe/jednolity-europejski-dokument-zamowienia>dostępna jest Instrukcja Wypełniania Jednolitego Europejskiego Dokumentu Zamówienia (w języku polskim).

***Jednolity Europejski Dokument Zamówienia (JEDZ) składa się w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.***

1. Dodatkowe oświadczenia składane obligatoryjnie wraz z ofertą:
	1. w przypadku wspólnego ubiegania się o zamówienie przez wykonawców, jednolity dokument (JEDZ), o którym mowa w ust. 1.1 powyżej składa każdy z wykonawców; ***Jednolity Europejski Dokument Zamówienia (JEDZ) składa się w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym;***
	2. wykonawcy wspólnie ubiegający się o zamówienie muszą dołączyć do oferty oświadczenie, z którego wynika, które dostawy wykonają poszczególni wykonawcy;
	3. wykonawcy polegający na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby wykonawcy muszą dołączyć do oferty:
		1. JEDZ podmiotu udostępniającego zasoby, potwierdzający brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby;
		2. zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, przy czym zobowiązanie, o którym mowa potwierdza, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:

a.1 zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;

a.2 sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;

a.3 czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

1. Dokumenty i oświadczenia składane przez wykonawcę na wezwanie zamawiającego – dotyczy wykonawcy najwyżej ocenionego w rankingu punktacji.
	1. Zamawiający wzywa wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż dziesięć (10) dni od dnia wezwania, podmiotowych środków dowodowych, tj.:
		1. wykazu dostaw, potwierdzającego spełnienie warunku podmiotowego udziału w postępowaniu, o którym mowa w rozdziale VI ust. 4.1 SWZ wraz z informacjami na temat przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane;
		2. dowodów określających czy dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy;
		3. informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 108 ust. 1 pkt. 1 i 2 ustawy PZP oraz w art. 108 ust. 1 pkt 4 ustawy PZP, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego – sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;
		4. oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej;
		5. zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków i opłat, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem podatków lub opłat wraz z zaświadczeniem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert wykonawca dokonał płatności należnych podatków lub opłat wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
		6. zaświadczenia albo innego dokumentu właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub właściwego oddziału regionalnego lub właściwej placówki terenowej Kasy Rolniczego Ubezpieczenia Społecznego potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne wraz z zaświadczeniem albo innym dokumentem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert wykonawca dokonał płatności należnych składek na ubezpieczenia społeczne lub zdrowotne wraz odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
		7. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, chyba że wykonawca wskazał w treści JEDZ dane umożliwiające dostęp do bezpłatnych i ogólnodostępnych baz danych, z których zamawiający może je uzyskać;
		8. oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu JEDZ złożonym do oferty, w zakresie podstaw do wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w art. 108 ust. 1 pkt 3, art. 108 ust. 1 pkt 4, art. 108 ust. 1 pkt 5, art. 108 ust. 1 pkt 6, art. 109 ust. 1 pkt 1, art. 109 ust. 1 pkt 5 i od 7 do 10 ustawy PZP.
2. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczpospolitej Polskiej, zamiast:
	1. informacji z Krajowego Rejestru Karnego, o której mowa w Rozdziale VIII ust. 3.1.4 powyżej – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania – wystawione nie wcześniej niż 6 miesięcy przed jego złożeniem,
	2. zaświadczenia albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, o których mowa w Rozdziale VIII ust. 3.1.7 powyżej, lub odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w ust. 3.1.8 powyżej – składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
* nie naruszył obowiązków dotyczących płatności podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne,
* nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury –

wystawione nie wcześniej niż 3 miesiące przed ich złożeniem.

* 1. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w rozdziale VIII ust. 4.1-4.2, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków z art. 108 ust. 1 pkt 1, 2 i 4, oraz w art. 109 ust. 1 pkt 1 ustawy, które wskazane są w rozdziale VII ust. 2 SWZ, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczeniem osoby, której dokument miał dotyczyć, złożonym pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożonym przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy. Zapisy dotyczące ważności dokumentów wskazane rozdziale VIII ust. 4.1 i 4.2 stosuje się odpowiednio.
1. W przypadku, gdy wykonawca polega na zasobach podmiotów udostępniających zasoby wykonawcy w celu wykazania spełnienia warunków udziału w postępowaniu, podmiotowe środki dowodowe winny zostać przedstawione przez ten podmiot w zakresie w jakim wykonawca powołuje się na jego zasoby.
2. Jeżeli wykonawca nie złożył JEDZ, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, zamawiający wzywa wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie nie krótszym niż dwa (2) dni robocze, chyba że oferta wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub zachodzą przesłanki unieważnienia postępowania.
3. Podmiotowe środki dowodowe sporządzone w języku obcym składa się wraz z tłumaczeniem na język polski.

**Rozdział IX – Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów wraz ze wskazaniem osób uprawnionych do kontaktów z wykonawcami**

1. Informacje ogólne dotyczące sposobu porozumiewania się zamawiającego z wykonawcami.
	1. W postępowaniu o udzielenie zamówienia komunikacja między zamawiającym a wykonawcami odbywa się przy użyciu miniPortalu <https://miniportal.uzp.gov.pl/>,ePUAPu <https://epuap.gov.pl/wps/portal> oraz poczty elektronicznej, z zastrzeżeniem, iż oferta musi zostać złożona przy użyciu miniPortalu.
	2. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.
	3. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, cyfrowego odwzorowania z dokumentem w postaci papierowej, oświadczeń oraz informacji przekazywanych z ich użyciem opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP.
	4. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do złożenia, zmiany, wycofania oferty lub wniosku oraz do komunikacji wynosi 150 MB.
	5. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
	6. Sposób sporządzenia i przekazania dokumentów elektronicznych oraz cyfrowego odwzorowania z dokumentem w postaci papierowej musi być zgody z wymaganiami określonymi w rozporządzeniu 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 (t.j.: Dz. U. 2020 r., poz. 2452 z późn. zm) oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (t. j.: Dz. U. 2020 r., poz. 2415 z późn. zm.), tj.:
		1. oferty, oświadczenia, o których mowa w art. 125 ust. 1 ustawy PZP, podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy PZP, oraz zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust. 3 cyt. ustawy, przedmiotowe środki dowodowe, pełnomocnictwo, 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 (tekst jednolity: Dz.U. z 2020 r. poz. 346 z późn. zm.).;
		2. informacje, oświadczenia lub dokumenty, inne niż określone w pkt 1.6.1 powyżej, przekazywane w postępowaniu o udzielenie zamówienia, 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 (tekst jednolity: Dz.U. z 2020 r. poz. 346 z późn. zm.), lub jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej, wskazanych przez zamawiającego w niniejszej SWZ;
		3. w szczególności, zamawiający podkreśla, że dokumenty lub oświadczenia, w tym oferta oraz dokumenty potwierdzające wniesienie wadium w formie innej niż pieniężna, składane są w oryginale ***w formie elektronicznej przy użyciu kwalifikowanego podpisu elektronicznego;***
		4. ***dokumenty wystawione w formie elektronicznej przekazuje się jako dokumenty elektroniczne, zapewniając zamawiającemu możliwość weryfikacji podpisów;***
		5. jeżeli oryginał dokumentu, oświadczenia lub inne dokumenty składane w postępowaniu o udzielenie zamówienia, nie zostały sporządzone w postaci dokumentu elektronicznego, wykonawca może sporządzić i przekazać cyfrowe odwzorowanie z dokumentem lub oświadczeniem w postaci papierowej, opatrując je kwalifikowanym podpisem elektronicznym, co jest równoznaczne z poświadczeniem przekazywanych dokumentów lub oświadczeń za zgodność z oryginałem;
		6. w przypadku przekazywania przez wykonawcę cyfrowego odwzorowania z dokumentem w postaci papierowej, opatrzenie go kwalifikowanym podpisem elektronicznym przez wykonawcę albo odpowiednio przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 118 ustawy PZP, albo przez podwykonawcę jest równoznaczne z poświadczeniem za zgodność z oryginałem.
	7. Zamawiający informuje, że identyfikator (ID) przedmiotowego postępowania dostępny jest na liście wszystkich postępowań zamieszczanych na miniPortalu i przyjmuje postać: f3469687-9842-4de5-a576-c642e8ac226f
2. Sposób porozumiewania się zamawiającego z wykonawcami w zakresie skutecznego złożenia oferty.
	1. Wykonawca składa ofertę za pośrednictwem ePUAPu, przy pomocy formularzy, o których mowa powyżej. Chwilą złożenia oferty jest czas na serwerze obsługującym miniPortal. Serwer zapisuje wysyłane na niego dane z dokładnością co do setnej części sekundy. ***Zamawiający zastrzega, iż złożenie oferty w innej formie niż elektroniczna będzie skutkować odrzuceniem oferty na podstawie art. 226 ust. 1 pkt 6 ustawy PZP.***
	2. Oferta musi być sporządzona z zachowaniem postaci elektronicznej w formacie danych ***.pdf, .doc, .docx, .rtf, .xps, .odt*** i podpisana kwalifikowanym podpisem elektronicznym. Sposób złożenia oferty, w tym jej zaszyfrowania/deszyfrowania opisany został w Regulaminie korzystania z miniPortal. Oferta musi być złożona w oryginale.
	3. Po upływie terminu składania ofert, wskazanego w rozdziale XIII SWZ wykonawca nie może skutecznie dokonać zmiany ani wycofać uprzednio złożonej oferty.
3. Sposób porozumiewania się zamawiającego z wykonawcami w zakresie skutecznego złożenia zawiadomień, dokumentów elektronicznych, oświadczeń lub cyfrowego odwzorowania z dokumentem w postaci papierowej oraz innych informacji składanych w przedmiotowym postępowaniu (nie dotyczy składania ofert).
	1. W postępowaniu o udzielenie zamówienia komunikacja pomiędzy zamawiającym
	a wykonawcami, a w szczególności składanie oświadczeń, wniosków (innych niż wskazane w ust. 2, zawiadomień oraz przekazywanie informacji odbywa się elektronicznie w dwojaki sposób:
4. za pośrednictwem dedykowanego formularza dostępnego na ePUAP oraz na miniPortalu (tzw. „Formularz do komunikacji”), przy czym przy wykorzystaniu niniejszego narzędzia zamawiający i wykonawca posługują się numerem ogłoszenia (BZP lub TED), ID postępowania bądź narzuconym znakiem sprawy

lub

1. za pomocą poczty elektronicznej (adres e-mail osoby wskazanej w ust. 4 poniżej).

***Wszelkie dokumenty składane zamawiającemu tytułem uzupełnienia bądź też wyjaśnień należy opatrywać podpisami, mimo korzystania z form komunikacji, o których mowa w niniejszym punkcie.***

1. Do porozumiewania z wykonawcami upoważniona w zakresie formalno-prawnym jest – *Piotr Molczyk, tel.: +4812 663-39-02, e-mail*.: piotr.molczyk@uj.edu.pl

**Rozdział X – Wymagania dotyczące wadium**

1. Zamawiający nie przewiduje konieczności wniesienia wadium.

**Rozdział XI – Termin związania ofertą**

1. Wykonawca jest związany złożoną ofertą od dnia upływu terminu składania ofert (włącznie) do dnia 16.04.2022 r.***.***
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą wraz z przedłużeniem okresu ważności wadium, bądź jeżeli jest to niemożliwe, wniesieniem nowego wadium na przedłużony okres związania ofertą.

**Rozdział XII – Opis sposobu przygotowania ofert**

1. Każdy wykonawca może złożyć tylko jedną ofertę na realizacji całości przedmiotu zamówienia.
2. Ofertę składa się z zachowaniem formy i sposobu opisanych w rozdziale IX niniejszej SWZ.
3. Dopuszcza się możliwość złożenia oferty przez dwa lub więcej podmiotów wspólnie ubiegających się o udzielenie zamówienia publicznego na zasadach opisanych w treści art. 58 ustawy PZP.
4. Oferta musi być napisana w języku polskim.
5. Oferta wraz ze wszystkimi jej załącznikami musi być podpisana przez osobę (osoby) uprawnioną do reprezentacji wykonawcy, zgodnie z wpisem do Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub do innego, właściwego rejestru. Jeżeli w imieniu wykonawcy działa osoba, której umocowanie nie wynika z ww. dokumentów, wykonawca wraz z ofertą przedkłada pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania wykonawcy. Pełnomocnictwa sporządzone w języku obcym wykonawca składa wraz z tłumaczeniem na język polski.
6. W przypadku składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia lub w sytuacji reprezentowania wykonawcy przez pełnomocnika do oferty musi być dołączone pełnomocnictwo. Wraz  z pełnomocnictwem winien być złożony dokument potwierdzający możliwość udzielania pełnomocnictwa.
7. Pełnomocnictwo przekazuje się w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym. Pełnomocnictwo sporządzone jako dokument w postaci papierowej i opatrzony własnoręcznym podpisem przekazuje się jako cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej, przy czym poświadczenia dokonuje mocodawca lub notariusz, zgodnie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. **–** Prawo o notariacie (Dz. U. 2020 r., poz. 1192 z późn. zm.).
8. Oferta wraz ze stanowiącymi jej integralną część załącznikami musi być sporządzona przez wykonawcę, wedle treści postanowień niniejszej SWZ i jej załączników, a w szczególności musi zawierać:
	1. formularz oferty wraz z załącznikami, w tym:
		1. Jednolity Europejski Dokument Zamówienia (JEDZ) w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym – w przypadku wykonawców wspólnie ubiegających się o zamówienie JEDZ składa każdy z nich;
		2. w przypadku podmiotu udostępniającego zasoby wykonawcy (o ile dotyczy), tj.:
9. JEDZ w zakresie, w jakim go dotyczy;
10. oświadczenie o udostępnieniu zasobów wykonawcy wraz ze stosownym zobowiązaniem lub innym środkiem dowodowym /o ile dotyczy/;
	* 1. pełnomocnictwo (zgodnie z ust. 5-7 powyżej) lub inny dokument potwierdzający umocowanie do reprezentowania wykonawcy;
		2. wykaz podwykonawców;
11. Jeżeli wykonawca zastrzega sobie prawo do nieudostępnienia innym uczestnikom postępowania informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, to składa w treści oferty stosowne oświadczenie zawierające wykaz zastrzeżonych dokumentów wraz z uzasadnieniem ich utajnienia. Dokumenty opatrzone klauzulą; „Dokument zastrzeżony” winny być załączone łącznie z ww. oświadczeniem, na końcu oferty. Wykonawca nie może zastrzec informacji, o których mowa w art. w art. 222 ust. 5 ustawy PZP.
12. Wszystkie koszty związane z przygotowaniem i złożeniem oferty ponosi wykonawca.

**Rozdział XIII – Miejsce oraz termin składania i otwarcia ofert**

1. Oferty należy składać w terminie ***do dnia 17 stycznia 2022 r., do godziny 09:00,*** na zasadach, opisanych w rozdziale IX ust. 2-3 SWZ.
2. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem formularza do wycofania oferty dostępnego na ePUAP i udostępnionego na miniPortalu. Sposób wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
4. Otwarcie ofert nastąpi ***w dniu 17 stycznia 2022 r., o godzinie 10:00*** za pomocą funkcjonalności „Deszyfrowanie” udostępnionej zamawiającemu w  miniPortalu, pod adresem <https://miniportal.uzp.gov.pl/>*.*
5. W przypadku awarii systemu teleinformatycznego, skutkującej brakiem możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
7. Zamawiający najpóźniej przed otwarciem ofert udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
8. Zamawiający niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
	1. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
	2. cenach lub kosztach zawartych w ofertach.
9. Zamawiający nie przewiduje przeprowadzania jawnej sesji otwarcia ofert z udziałem wykonawców, jak też transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line.

**Rozdział XIV – Opis sposobu obliczania ceny**

1. Cenę oferty należy podać w PLN i wyliczyć w oparciu o indywidualną kalkulację z podaniem cen jednostkowych, przy uwzględnieniu wymagań i zapisów ujętych w niniejszej SWZ i jej załącznikach oraz przy uwzględnieniu rabatów, opustów, itp., których wykonawca zamierza udzielić.
2. Nie przewiduje się żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu umowy.
3. W przypadku złożenia oferty przez wykonawcę nie zobowiązanego, bądź zwolnionego z obowiązku odprowadzania podatku od towarów i usług VAT, podczas czynności porównania ofert, zamawiający doliczy do zaoferowanej przez ww. wykonawcę ceny stosowny podatek, do uiszczenia którego będzie obowiązany. W tym wypadku koszt podatku pokrywa zamawiający.
4. Ceny muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.
6. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
7. W czasie obowiązywania zawartej z wyłonionym wykonawcą umowy wysokość maksymalnego wynagrodzenia należnego wykonawcy może ulec zmianie w drodze pisemnego aneksu w przypadkach opisanych w treści załączonego do niniejszej SWZ wzoru umowy.

**Rozdział XV – Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty wraz z podaniem ich znaczenia i sposobu oceny ofert**

1. Kryteria oceny ofert i ich znaczenie:
	1. Cena ryczałtowa brutto za całość zamówienia – **70%**
	2. Wspólne środowisko GUI dla całości wdrażanego systemu (poza firewallem): – **30%**
2. Punkty przyznawane za kryterium „cena ryczałtowa za całość zamówienia” będą liczone wg następującego wzoru:

**C = (Cnaj : Co) x 10**

gdzie:

C – liczba punktów przyznana danej ofercie,

Cnaj – najniższa cena spośród ważnych ofert,

Co – cena podana przez Wykonawcę dla którego wynik jest obliczany.

Maksymalna liczba punktów, które Wykonawca może uzyskać, wynosi 10.

1. Punkty przyznawane za kryterium „Wspólne środowisko GUI dla całości wdrażanego systemu (poza firewallem)” będą przyznawane w następujący sposób:
* Wspólne środowisko GUI dla całości wdrażanego systemu (poza firewallem) **– 10 punktów**
* Brak wspólnego środowiska GUI dla całości wdrażanego systemu (poza firewallem) **– 0 punktów**

Maksymalna liczba punktów, które Wykonawca może uzyskać wynosi 10.

1. Po dokonaniu ocen, punkty przyznane dla każdego z kryteriów zostaną przemnożone przez wagi przyjętych kryteriów i zsumowane.
2. Suma ta stanowić będzie końcową ocenę danej oferty.
3. Wszystkie obliczenia punktów będą dokonywane z dokładnością do dwóch miejsc po przecinku (bez zaokrągleń).
4. Oferta Wykonawcy, która uzyska najwyższą sumaryczną liczbę punktów, uznana zostanie za najkorzystniejszą.
5. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
6. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, zamawiający wybiera ofertę z najniższą ceną lub najniższym kosztem.
7. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa w ust. 2, zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych zawierających nową cenę lub koszt.

**Rozdział XVI – Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego**

1. Przed podpisaniem umowy wykonawca powinien złożyć:

1.1 kopię umowy(-ów) określającej podstawy i zasady wspólnego ubiegania się o udzielenie zamówienia publicznego – w przypadku złożenia oferty przez podmioty występujące wspólnie (tj. konsorcjum);

1.2 wykaz podwykonawców z zakresem powierzanych im zadań, o ile przewiduje się ich udział w realizacji zamówienia.

1. Wybrany wykonawca jest zobowiązany do zawarcia umowy w terminie i miejscu wyznaczonym przez zamawiającego.

**Rozdział XVII – Wymagania dotyczące zabezpieczenia należytego wykonania umowy**

1. Zamawiający nie przewiduje konieczności wniesienia zabezpieczenia należytego wykonania umowy.

**Rozdział XVIII – Wzór umowy /projektowane postanowienia umowne/ – załącznik nr 2 do SWZ.**

**Rozdział XIX – Pouczenie ośrodkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia publicznego**

1. Środki ochrony prawnej przysługują wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł́ lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy PZP.
2. 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 której́ zamawiający był obowiązany̨ na podstawie ustawy PZP.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o któryḿ mowa w art. 519 ust. 1 ustawy PZP, stronom oraz uczestnikom postepowania odwoławczego przysługuje skarga do sadu. Skargę̨ wnosi się, do Sądu Okręgowego w Warszawie – sądu zamówień publicznych za pośrednictweḿ Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” ustawy PZP.

**Rozdział XX – Postanowienia ogólne**

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Powody niedokonania podziału zamówienia na części: *ze względu na specyfikę zamówienia oraz konieczność zapewnienia kompleksowej obsługi świadczonej przez jednego wykonawcę, a także możliwość uzyskania lepszych cen i efektów przy udzieleniu zamówienia o większym zakresie przedmiotowym.*
3. Zamawiający nie przewiduje zawarcia umowy ramowej.
4. Zamawiający nie przewiduje możliwości udzielenie zamówienia polegającego na powtórzeniu podobnych dostaw na podstawie art. 214 ust. 1 pkt 7 ustawy PZP.
5. Zamawiający nie dopuszcza składania ofert wariantowych.
6. Rozliczenia pomiędzy wykonawcą a zamawiającym będą dokonywane w złotych polskich (PLN).
7. Zamawiający nie przewiduje aukcji elektronicznej.
8. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
9. Zamawiający żąda wskazania w ofercie przez wykonawcę tej części zamówienia, odpowiednio do treści postanowień SWZ, której wykonanie zamierza powierzyć podwykonawcom, a także wskazania nazw (firm) podwykonawców na zasoby, których się powołuje w celu spełnienia warunków udziału w postępowaniu.

**Rozdział XXI – Informacje o przetwarzaniu danych osobowych – dotyczy wykonawcy będącego osobą fizyczną**

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej „RODO”) w zw. z art. 19 ust. 1 ustawy PZP, Uniwersytet Jagielloński informuje, że:

* + - 1. **Administratorem** Pani/Pana danych osobowych jest Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków, reprezentowany przez Rektora UJ.
			2. **Uniwersytet Jagielloński wyznaczył Inspektora Ochrony Danych**, ul. Gołębia 24, 31-007 Kraków, pokój nr 5. Kontakt z Inspektorem możliwy jest przez e-mail: iod@uj.edu.pl lub pod nr telefonu +4812 663 12 25.
			3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c) RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego*, nr sprawy* **80.272.253.2021.**
			4. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy PZP związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.
			5. Konsekwencje niepodania danych osobowych wynikają z ustawy PZP.
			6. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 3 oraz 4 ustawy PZP, przy czym udostepnieniu nie podlegają dane osobowe, o których mowa w art. 9 ust. 1 RODO, zebrane w toku postępowania o udzielenie zamówienia.
			7. Pani/Pana dane osobowe będą przechowywane zgodnie z art. 78 ust. 1 ustawy PZP przez okres co najmniej 4 lat liczonych od dnia zakończenia postępowania o udzielenie zamówienia publicznego albo do upływu terminu możliwości kontroli projektu współfinansowanego lub finansowanego ze środków Unii Europejskiej albo jego trwałości takie projektu bądź innych umów czy zobowiązań wynikających z realizowanych projektów.
			8. Posiada Pani/Pan prawo do:
1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
2. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
3. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych,
4. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
	* + 1. Nie przysługuje Pani/Panu prawo do:
5. prawo do usunięcia danych osobowych w zw. z art. 17 ust. 3 lit. b), d) lub e) RODO,
6. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
7. prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c) w zw. z art. 21 RODO.
	* + 1. **Pana/Pani dane osobowe, o których mowa w art. 10 RODO**, mogą zostać udostępnione, w celu umożliwienia korzystania ze środków ochrony prawnej, o których mowa w Dziale IX ustawy PZP, do upływu terminu na ich wniesienie.
			2. Zamawiający informuje, że **w odniesieniu do Pani/Pana danych osobowych** decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
			3. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 – 3 RODO, celem realizacji Pani/Pana uprawnienia wskazanego pkt 8 lit. a) powyżej, wymagałoby niewspółmiernie dużego wysiłku, **zamawiający może żądać od Pana/Pani**, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty wszczętego albo zakończonego postępowania o udzielenie zamówienia publicznego.
			4. **Skorzystanie przez Panią/Pana**, z uprawnienia wskazanego pkt 8 lit. b) powyżej, do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 RODO, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego, ani zmianą postanowień umowy w zakresie niezgodnym z ustawą PZP, ani nie może naruszać integralności protokołu postępowania o udzielenie zamówienia publicznego oraz jego załączników.
			5. **Skorzystanie przez Panią/Pana**, z uprawnienia wskazanego pkt 8 lit. c) powyżej,polegającym nażądaniu ograniczenia przetwarzania danych, o którym mowa w art. 18 ust. 1 Rozporządzenia Ogólnego, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego oraz również po postępowania w przypadku wystąpienia okoliczności, o których mowa w art. 18 ust. 2 RODO (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).

**Rozdział XXII – Załączniki do SWZ**

1. **Załącznik A do SWZ – Opis przedmiotu zamówienia**
2. **Załącznik nr 1 – Formularz oferty;**
3. **Załącznik nr 2 – Wzór umowy (projektowane postanowienia umowne).**

**FORMULARZ OFERTY – Znak sprawy 80.272.253.2021**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*ZAMAWIAJĄCY:* ***Uniwersytet Jagielloński***

***ul. Gołębia 24, 31 – 007 Kraków*;**

*Jednostka prowadząca sprawę:* ***Dział Zamówień Publicznych UJ***

***ul. Straszewskiego 25/3 i 4, 31-113 Kraków***

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Nazwa (Firma) wykonawcy:*

................................................................................

................................................................................

*Adres siedziby:*

................................................................................

................................................................................

*Adres do korespondencji:*

................................................................................

................................................................................

*Kontakt:*

*tel.:* ...................................................................

*fax:* ...................................................................

 *e-mail:* ...................................................................

*Inne dane:*

*NIP*: .............................................................

*REGON*: ...............................................................

*Nawiązując do ogłoszonego przetargu nieograniczonego zakresie dostawy sprzętu komputerowego oraz oprogramowania wraz z montażem w ramach modernizacji infrastruktury sieciowej przewodowej oraz bezprzewodowej w budynku Wydziału Biochemii, Biofizyki i Biotechnologii Uniwersytetu Jagiellońskiego, składamy poniższą ofertę:*

oferujemy wykonanie całości przedmiotu zamówienia za łączną ***kwotę netto .......................................... PLN,*** *(słownie: .................................................................. zł ……/100)* plus należny podatek VAT w wysokości ***…… %,*** co daje ***kwotę brutto ................................................ PLN*** *(słownie: .......................................................... zł ……/100)\*;*

*w tym:* *switche, kontrolery sieciowe, routery sieci wifi, serwery, zapory sieci*

*za kwotę netto .......................................... PLN, (słownie: .................................................................. zł ……/100) plus należny podatek VAT w wysokości …… %, co daje kwotę brutto ................................................ PLN*

oferujemy termin płatności zgodny z wymaganiami określonymi w § 4 wzoru umowy (projektowanych postanowień umowy);

oświadczamy, iż oferujemy przedmiot zamówienia zgodny z wymaganiami i warunkami określonymi przez zamawiającego w specyfikacji warunków zamówienia oraz w ustawie PZP;

oświadczamy, iż oferujemy termin realizacji zamówienia określony w rozdziale V SWZ;

oświadczamy, że wybór oferty:

* nie będzie prowadził do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy o podatku od towarów i usług\*
* będzie prowadził do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy o podatku od towarów i usług. Powyższy obowiązek podatkowy będzie dotyczył *……………………………………………………………………..………….*

*…………………………………………………………………………………………………….\**

*[\*1/niepotrzebne skreślić; 2/wpisać nazwę/rodzaj towaru lub usługi, które będą prowadziły do powstania u zamawiającego obowiązku podatkowego, zgodnie z przepisami obowiązującej ustawy o podatku od towarów i usług VAT]*

oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w rozdziale XI specyfikacji warunków zamówienia;

oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WEwobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu;

w przypadku przyznania nam zamówienia – zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez zamawiającego;

osobą upoważnioną do kontaktów z zamawiającym w zakresie złożonej oferty oraz w sprawach związanych z realizacją zamówienia jest: ……………………………………………………….

*[\*wypełnić dane personalne i adresowe – tel.; e-mail]*

oferta liczy **........................\*** kolejno ponumerowanych kart;

załącznikami do niniejszego formularza są:

* *Załącznik nr 1*– JEDZ;
* *Załącznik nr 2*– kalkulacja cenowa oferty, sporządzona z uwzględnieniem wytycznych opisanych w treści SWZ oraz treści załącznika A do SWZ;
* *Załącznik nr 3 –* oświadczenie dotyczące podmiotu udostępniającego zasoby wykonawcy/ (o ile dotyczy), tj.:
* JEDZ w zakresie w jakim go dotyczy;
* oświadczenie o udostępnieniu zasobów wykonawcy wraz ze stosownym zobowiązaniem lub innym środkiem dowodowym (o ile dotyczy);
* *Załącznik nr 4* – oświadczenie o powierzeniu podwykonawcom wykonania części przedmiotu zamówienia (Wykaz podwykonawców – o ile dotyczy);
* Inne.

**Załącznik nr 1 do formularza oferty – JEDZ**

**Załącznik nr 2 do formularza oferty –**

***Szczegółowa kalkulacja cenowa, sporządzona z uwzględnieniem danych zawartych w załączniku A do SWZ /tabela z załącznika A/***

**Załącznik 3 do formularza oferty**

**OŚWIADCZENIE**

**DOTYCZĄCE PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY WYKONAWCY**

***[należy przedstawić dla każdego podmiotu udostępniającego zasoby wykonawcy oddzielnie – oświadczenie składane przez podmiot udostępniający]***

|  |  |
| --- | --- |
| Nazwa  | ...................................................................... |
| Adres  | ...................................................................... |
|  |  |

Ja (My) niżej podpisany (ni)

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

działając w imieniu i na rzecz : ……………………………………………………………………………………………………………

w związku tym, iż wykonawca:

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

*[pełna nazwa wykonawcy i adres/siedziba wykonawcy]*

**Oświadczam, że:**

* + 1. **zobowiązuję się udostępnić swoje zasoby ww. wykonawcy.**

W celu oceny, czy ww. wykonawca będzie dysponował moimi zasobami w stopniu niezbędnym dla należytego wykonania zamówienia oraz oceny, czy stosunek nas łączący gwarantuje rzeczywisty dostęp do moich zasobów podaję następujące informacje:

1. zakres moich zasobów dostępnych wykonawcy:

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

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

1. sposób wykorzystania moich zasobów przez wykonawcę przy wykonywaniu zamówienia:

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

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

1. charakteru stosunku, jaki będzie mnie łączył z wykonawcą:

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

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

1. zakres i okres mojego udziału przy wykonywaniu zamówienia:

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

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

* + 1. **spełniam warunki udziału w postępowaniu w zakresie, w którym mnie dotyczą – zgodnie z JEDZ.**

**Załącznik 4 do formularza oferty**

**OŚWIADCZENIE**

***(wykaz podwykonawców)***

Oświadczamy, że:

* powierzamy\* następującym podwykonawcom wykonanie następujących części (zakresu) zamówienia:
1. Podwykonawca: ………………………………………………………………………………..

*[\*podać: pełną nazwę/firmę; adres; w zależności od podmiotu: NIP/PESEL, numer KRS/CEIDG]*

Zakres zamówienia ……………………………………………………………………………..

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

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

*[\*podać]*

1. Podwykonawca: ………………………………………………………………………………..

*[\*podać: pełną nazwę/firmę; adres; w zależności od podmiotu: NIP/PESEL, numer KRS/CEIDG]*

Zakres zamówienia …………………………………………………………………………..…

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

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

*[\*podać]*

* nie powierzamy\* podwykonawcom żadnej części (zakresu) zamówienia

*[\*w razie braku podwykonawców – niepotrzebne skreślić]*

 ***[Jeżeli wykonawca nie wykreśli żadnej z powyższych opcji, zamawiający uzna, że nie powierza podwykonawcom wykonania żadnych prac objętych przedmiotowym zamówieniem]***

**Załącznik nr 2 do SWZ**



**UMOWA 80.272.253.2021 – wzór /projektowane postanowienia umowy/**

***zawarta w Krakowie w dniu ...................... pomiędzy:***

***Uniwersytetem Jagiellońskim z siedzibą w Krakowie przy ul. Gołębiej 24, reprezentowanym przez:***

***zwanym dalej w treści umowy „Zamawiającym”***

***a***

***.............................................................................................................z siedzibą w ........................... reprezentowanym przez ......................................................................................***

***zwanym dalej w treści umowy „Wykonawcą”.***

*Niniejsza umowa jest wynikiem przeprowadzonego postępowania o udzielenie zamówienia publicznego w* ***trybie przetargu nieograniczonego****, na podstawie art. 132 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j.: Dz.U. z 2019 r., poz. 2019 z późn zm.; tj. Dz.U. z 2021 r., poz. 1129 z późn. zm.), zwanej dalej „ustawą PZP”.*

§ 1

Przedmiotem umowy jest dostawa i montaż sprzętu komputerowego wraz z oprogramowaniem, zwanego dalej „sprzętem lub „aparaturą”, w ramach modernizacji infrastruktury sieciowej przewodowej oraz bezprzewodowej w budynku Wydziału Biochemii, Biofizyki i Biotechnologii Uniwersytetu Jagiellońskiego, z siedzibą w Krakowie, przy ul……………...

1. Przedmiot niniejszej umowy, określony w ust. 1, obejmuje również szkolenie administratorów z zainstalowanych systemów w wymiarze min. 30 godzin zegarowych, w miejscu instalacji lub zdalnie jeżeli będzie to możliwe.
2. Zakres dostaw w tym rodzaj i ilość aparatury, rodzaj czynności i prac objętych niniejszą umową określony jest szczegółowo w ofercie Wykonawcy z dnia …………. oraz w dokumentacji postępowania przetargowego, w szczególności w Specyfikacji Warunków Zamówienia oraz Załączniku A do SWZ, będącymi integralną częścią niniejszej umowy.
3. Zamawiający zleca, a Wykonawca zobowiązuje się wykonać wszelkie niezbędne czynności dla zrealizowania przedmiotu umowy.
4. Wykonawca oświadcza, że znana jest mu sytuacja społeczno-gospodarcza zaistniała w dniu złożenia oferty w postępowaniu o udzielenie niniejszego zamówienia publicznego oraz w dniu zawarcia niniejszej Umowy, a ewentualne ryzyko związane z niedostępnością zaoferowanego modelu sprzętu komputerowego lub koniecznością zaoferowania modelu o nie gorszych parametrach technicznych niż w modelu objętym umową wkalkulował w cenę oferty, w tym cenę jednostkową oferowanego sprzętu komputerowego.
5. Zamawiający zleca, a Wykonawca zobowiązuje się wykonać wszelkie niezbędne dostawy i czynności dla zrealizowania przedmiotu umowy w terminie **12 miesięcy**, licząc od dnia zawarcia niniejszej umowy.
6. Integralną częścią niniejszej umowy są:

a) dokumentacja postępowania przetargowego wraz z ofertą Wykonawcy;

b) lista podwykonawców z określeniem zakresu i wartości robót przewidzianych do wykonania (załącznik nr 1), o ile są przewidziani na etapie zawarcia umowy.

§ 2

* + - 1. Wykonawca oświadcza, że posiada odpowiednią wiedzę, doświadczenie i dysponuje stosowną bazą do wykonania przedmiotu umowy oraz zobowiązuje się wykonać przedmiot umowy przy zachowaniu należytej staranności uwzględniając zawodowy charakter prowadzonej przez Wykonawcę działalności.
			2. Wykonawca oświadcza, iż przedmiot umowy wykona z zachowaniem wysokiej jakości użytych materiałów i wykonywanych prac oraz dotrzyma umówionych terminów, przy zachowaniu należytej staranności, uwzględniając zawodowy charakter prowadzonej przez niego działalności.
			3. Wykonawca oświadcza i gwarantuje, iż dochowane zostaną przez niego wszelkie parametry oraz wymagania i warunki techniczne, funkcjonalne i jakościowe opisane w SWZ oraz w Załącznikach, a także w ofercie Wykonawcy.
			4. Wykonawca oświadcza, iż dostarczany sprzęt stanowiący przedmiot niniejszej umowy jest fabrycznie nowy (tj. nieregenerowany, nienaprawiany, niefabrykowany, nieużywany we wcześniejszych wdrożeniach), kompletny (w szczególności ze wszystkimi podzespołami, częściami, materiałami niezbędnymi do uruchomienia i użytkowania), jego zakup i korzystanie z niego zgodnie z przeznaczeniem, nie narusza prawa, w tym praw osób trzecich, a w zakresie bezpieczeństwa odpowiada normom CE w zakresie bezpieczeństwa urządzeń elektrycznych oraz posiada certyfikaty wskazane w SWZ, na potwierdzenie czego wraz z dostawą sprzętów, dołączy certyfikat lub inny dokument potwierdzający spełnienie ww. wymagań określonych w SWZ dla poszczególnej aparatury.
			5. Wykonawca zobowiązuje się do zapewnienia porządku w rejonie prowadzonych prac oraz wykonania niezbędnych zabezpieczeń w sposób gwarantujący bezpieczeństwo osób postronnych, co zostało skalkulowane w ryczałtowej cenie oferty. Wykonawca odpowiada za szkodę wyrządzoną osobom trzecim pozostającą w związku z wykonywaniem umowy.
			6. W ramach niniejszej umowy i wynikającego z niej wynagrodzenia Wykonawcy, wskazanego w § 4 ust. 2 umowy, Zamawiający nabywa nieodwołalne i nieograniczone czasowo prawo do korzystania ze wszelkiego oprogramowania niezbędnego do prawidłowego funkcjonowania przedmiotu umowy w zakresie wskazanym w art. 75 ust. 2 ustawy z dnia 04 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. 2019 poz. 1231 ze zm.), to jest na następujących polach eksploatacji:
1. sporządzenie kopii zapasowej, jeżeli jest to niezbędne do korzystania
z programu komputerowego. Jeżeli umowa nie stanowi inaczej, kopia ta nie może być używana równocześnie z programem komputerowym;
2. obserwowanie, badanie i testowanie funkcjonowania programu komputerowego w celu poznania jego idei i zasad przez osobę posiadającą prawo korzystania
z egzemplarza programu komputerowego, jeżeli, będąc do tych czynności upoważniona, dokonuje ona tego w trakcie wprowadzania, wyświetlania, stosowania, przekazywania lub przechowywania programu komputerowego;
3. zwielokrotnianie kodu lub tłumaczenie jego formy w rozumieniu art. 74 ust. 4 pkt 1 i 2 ww. ustawy, jeżeli jest to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania niezależnie stworzonego programu komputerowego z innymi programami komputerowymi, o ile zostaną spełnione następujące warunki:
4. czynności te dokonywane są przez Zamawiającego lub inną osobę uprawnioną do korzystania z egzemplarza programu komputerowego bądź przez inną osobę działającą na ich rzecz,
5. informacje niezbędne do osiągnięcia współdziałania nie były uprzednio łatwo dostępne dla osób, o których mowa pod lit. ca),
6. czynności te odnoszą się do tych części oryginalnego programu komputerowego, które są niezbędne do osiągnięcia współdziałania.
	* + 1. Wykonawca udziela licencji niewyłącznej, tj. prawa do korzystania z oprogramowania w zakresie wskazanym w niniejszym paragrafie umowy, w chwili podpisania protokołu odbioru, bez zastrzeżeń oraz zapłaty wynagrodzenia, o którym mowa w § 4 ust. 2 umowy, bez konieczności składania przez Strony dodatkowego oświadczenia woli.
			2. Przy odbiorze Wykonawca zobowiązany jest dostarczyć Zamawiającemu również egzemplarze oprogramowania stanowiące z dniem udzielenia ww. licencji własność Zamawiającego, w wersjach instalacyjnych albo wskazać adres strony internetowej z której ww. oprogramowanie można pobrać.

§ 3

Przedmiot umowy będzie realizowany przez Wykonawcę siłami własnymi/siłami własnymi i przy pomocy podwykonawców. Strony ustalają, że zgodnie z ofertą złożoną przez Wykonawcę, Wykonawca zleci niżej wymienionym podwykonawcom, następujące usługi ……………………………..….

Zlecenie wykonania części przedmiotu umowy podwykonawcom nie zmienia zobowiązania Wykonawcy względem Zamawiającego za należyte wykonanie tej części.

Wykonawca jest odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców w takim samym stopniu, jak za działania, uchybienia i zaniedbania własne.

Wykonawca ponosi całkowitą odpowiedzialność materialną i prawną za powstałe u Zamawiającego, jak i osób trzecich, szkody powstałe w związku z wykonywaniem niniejszej umowy, niezależnie od tego, czy szkoda powstała z powodu winy Wykonawcy. Wykonawca jest zobowiązany przed dokonaniem odbioru przedmiotu umowy do naprawienia wszelkich szkód wynikłych w związku z realizacją niniejszej umowy.

Jeśli Wykonawca w toku postępowania o udzielenie zamówienia publicznego w wyniku, którego zawarto niniejszą umowę, powoływał się na zasoby innych podmiotów będących jego podwykonawcami, w zakresie wskazanym w art. 118 ust. 1 ustawy PZP, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać, że proponowany inny podwykonawca lub on samodzielnie spełnia je w stopniu nie mniejszym niż określony w SWZ. Wykonawca zobowiązany jest do wykazania, że nowy podmiot trzeci lub podwykonawca nie podlega wykluczeniu z postepowania lub on samodzielnie spełnia je w stopniu nie mniejszym niż określony w SWZ.

§ 4

1. Wysokość wynagrodzenia przysługującego Wykonawcy za wykonanie przedmiotu umowy ustalona została na podstawie złożonej oferty i ma charakter ryczałtowy, nie podlega waloryzacji oraz uwzględnia w szczególności wszystkie koszty wykonania wszelkich usług i dostaw, niezbędnych do wykonania przedmiotu umowy, transportu i montażu nowych urządzeń, gwarancji oraz należny podatek od towarów i usług VAT, naliczony według aktualnie obowiązujących przepisów prawa oraz koszty oprogramowanie niezbędnego do prawidłowego funkcjonowania przedmiotu umowy.
2. Wynagrodzenie za przedmiot umowy wynosi kwotę netto …………… PLN, (słownie: ……………………. złotych …/100), która po doliczeniu obowiązującej stawki podatku od towarów i usług VAT daje kwotę brutto: ……………………. PLN, (słownie: ………………………….. złotych …/100), w tym switche, kontrolery sieciowe, routery sieci wifi, serwery, zapory sieci - kwotę netto .......................................... PLN, (słownie: .................................................................. zł ……/100) plus należny podatek VAT w wysokości …… %, co daje kwotę brutto ................................................ PLN
3. Strony zastrzegają, iż ceny jednostkowe za poszczególne sprzęty komputerowe wchodzące w skład przedmiotu umowy nie ulegną zmianie podczas trwania niniejszej umowy.
4. Zamawiający oświadcza, iż zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. 2021 poz. 685 ze zm.), zwana dalej „p.t.u.” będzie ubiegał się o zgodę na zastosowanie 0% stawki podatku od towarów i usług VAT na zamawiany sprzęt komputerowy w zakresie objętym ww. stawką podatkową – zgodnie z art. 83 ust. 1 pkt 26 przywołanej ustawy.
5. Wykonawca w ciągu 14 dni od otrzymania zawiadomienia Zamawiającego przesłanego na adres poczty elektronicznej Wykonawcy o wydaniu zaświadczenia przez ministra właściwego ds. szkolnictwa wyższego, potwierdzającego przeznaczenie dostarczonego sprzętu komputerowego dla placówki oświatowej w rozumieniu art. 83 ust. 1 pkt 26 p.t.u., wystawi i doręczy Zamawiającemu wystawioną korektę faktury opiewającą na kwotę netto wskazaną w § 5 ust. 2 umowy w zakresie objętym stawką 0% VAT do siedziby Działu Zaopatrzenia - Sekcji Aparatury UJ w Krakowie (30-060) przy ul. Ingardena 3, pokój nr 5. Postanowienia zdania pierwszego nie stosuje się w przypadku, gdy Wykonawca wystawił fakturę opiewającą na kwotę wynagrodzenia netto w zakresie objętym stawką 0% VAT. Wykonawca dokona zwrotu należności wskazanej w powyższej fakturze korygującej na wskazany przez Zamawiającego rachunek bankowy w terminie do 21 dni, licząc od dnia jej wystawienia.
6. Zamawiający jest podatnikiem VAT i posiada NIP 675-000-22-36.
7. Wykonawca jest podatnikiem VAT i posiada NIP …............................. lub nie jest płatnikiem VAT na terytorium Rzeczpospolitej Polskiej.
8. Należny od kwoty wynagrodzenia podatek od towarów i usług VAT, pokryje Zamawiający na konto właściwego Urzędu Skarbowego w przypadku powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.

§ 5

Wykonawca otrzyma wynagrodzenie po wykonaniu całości przedmiotu umowy (wszystkich dostaw i usług objętych przedmiotem umowy) potwierdzonym protokołem odbioru bez zastrzeżeń i po złożeniu prawidłowo wystawionej faktury w siedzibie jednostki organizacyjnej wskazanej w §1 ust. 1 umowy.

Strony zgodnie postanawiają, że datą zakończenia realizacji przedmiotu umowy (data wykonania) jest data podpisania protokołu odbioru końcowego, o którym mowa w ust.1

Termin zapłaty faktury za wykonany i odebrany przedmiot umowy ustala się do 30 dni od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury, po odebraniu przedmiotu umowy i po podpisaniu protokołu odbioru bez zastrzeżeń.

Faktura winna być wystawiana w następujący sposób:

**Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków,**

**NIP: 675-000-22-36, REGON: 000001270**

i opatrzona dopiskiem, dla jakiej Jednostki Zamawiającego zamówienie zrealizowano.

Wynagrodzenie przysługujące Wykonawcy jest płatne przelewem z rachunku Zamawiającego, na konto Wykonawcy wskazane na fakturze.

Miejscem płatności jest Bank Zamawiającego, a zapłata następuje w dniu zlecenia przelewu przez Zamawiającego.

Wykonawca zobowiązany jest do wskazania na fakturze numeru rachunku rozliczeniowego, który został ujawniony w wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT prowadzonym przez Szefa Krajowej Administracji Skarbowej (tzw. „Biała lista” – art. 96b ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług – t. j. Dz. U. 2020 poz. 106 ze zm.).

* 1. W razie braku ujawnienia bankowego rachunku rozliczeniowego Wykonawcy na „Białej liście”, Zamawiający będzie uprawniony do zapłaty wynagrodzenia na rachunek wskazany w fakturze, jednakże z jednoczesnym wypełnieniem obowiązków wynikających z obowiązujących przepisów prawa, w tym powiadomienia organów Krajowej Administracji Skarbowej.
	2. Zamawiający w przypadku, gdy Wykonawca jest zarejestrowany jako czynny podatnik podatku od towarów i usług Zamawiający może dokonać płatności wynagrodzenia z zastosowaniem mechanizmu podzielonej płatności, to jest w sposób wskazany w art. 108a ust. 2 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. 2020 poz. 106 ze zm.). Postanowień zdania 1. nie stosuje się, gdy przedmiot umowy stanowi czynność zwolnioną z podatku VAT albo jest on objęty 0% stawką podatku VAT.
	3. Wykonawca potwierdza, iż ujawniony na fakturze bankowy rachunek rozliczeniowy służy mu dla celów rozliczeń z tytułu prowadzonej przez niego działalności gospodarczej, dla którego prowadzony jest rachunek VAT.

§ 6

1. Zamawiający przystąpi do czynności odbioru przedmiotu umowy po pisemnym powiadomieniu go przez Wykonawcę o gotowości do odbioru. Dokument zgłoszenia o gotowości do odbioru Wykonawca zobowiązany jest dostarczyć do osoby wskazanej w § 14 ust.1.1 umowy na 3 dni robocze przed planowanym terminem odbioru. Wszystkie dostawy i czynności oraz ich odbiory muszą zakończyć się w terminie wykonania umowy określonym w § 1 ust. 6 niniejszej umowy.
2. Zamawiający dokona odbioru przedmiotu umowy w terminie 7 dni roboczych od dnia otrzymania przez niego pisemnego zawiadomienia Wykonawcy wskazanego w ust. 1 niniejszego paragrafu, pod warunkiem, iż przedmiot umowy będzie wolny od wad.
3. W przypadku, gdy w trakcie przeprowadzenia czynności odbiorowych przedstawiciele Zamawiającego stwierdzą, że przedmiot umowy po jego montażu i sprawdzeniu działania okaże się wadliwy Wykonawca zobowiązany jest do jego naprawy lub wymiany na swój koszt, zgodnie z zasadami odpowiedzialności z tytułu gwarancji.
4. Protokół odbioru przedmiotu umowy będzie sporządzony z udziałem upoważnionych przedstawicieli stron umowy, po sprawdzeniu zgodności realizacji przedmiotu umowy zgodnie z warunkami umowy, SWZ i ofertą Wykonawcy oraz po przekazaniu wymaganych SWZ certyfikatów oraz oświadczenia gwaranta, zawarte w szczególności w kartach gwarancyjnych producenta/ów wyposażenia, instrukcjach obsługi i eksploatacji.
5. Protokół odbioru całości przedmiotu umowy wskazany w ust. 2 niniejszego paragrafu umowy będzie zawierał w szczególności:
	1. wskazanie zbadanych elementów świadczenia przedmiotu umowy;
	2. zgodność świadczenia przedmiotu umowy z wymaganiami Zamawiającego opisanymi w SWZ;
	3. potwierdzenie możliwości bezpiecznej i zgodnej z SWZ eksploatacji świadczenia przedmiotu umowy;
	4. potwierdzenie sprawnego działania świadczenia przedmiotu umowy;
	5. potwierdzenie kompletności dokumentacji dostarczonej dla świadczenia przedmiotu umowy;
	6. oświadczenie o niestwierdzeniu wad fizycznych lub ewentualne wskazanie stwierdzonych wad fizycznych w świadczeniu przedmiotu umowy.
6. Dostawa części (urządzeń, elementów) składających się na przedmiot umowy nie jest równoznaczna z przekazaniem go do eksploatacji. Protokół odbioru przedmiotu umowy do eksploatacji może być podpisany dopiero po wykonaniu wszystkich dostaw i usług objętych umową.
7. Za dzień odbioru przedmiotu umowy Strony uważać będą dzień faktycznej realizacji przez Wykonawcę czynności i dostaw składających się na przedmiot zamówienia, który zostanie odnotowany ww. protokole.
8. Strony ustalają, że zostaną podpisane dwa oryginalne protokoły odbioru – jeden dla Zamawiającego i jeden dla Wykonawcy. Podpisanie takiego protokołu (bez stwierdzonych uwag) przez przedstawiciela Zamawiającego oraz przedstawiciela Wykonawcy uważane będzie za wykonanie świadczenia przedmiotu umowy.
9. Odbiór przedmiotu umowy nie wyłącza roszczeń Zamawiającego z tytułu nienależytego wykonania umowy, w szczególności w przypadku wykrycia wad przedmiotu umowy przez Zamawiającego po dokonaniu odbioru.

§ 7

* 1. Wykonawca zobowiązuje się wykonać przedmiot umowy bez wad (usterek), przy czym jest zobowiązany zweryfikować zgodność znajdujących się na przedmiocie umowy oznaczeń z danymi zawartymi w dokumencie gwarancyjnym (oświadczeniu gwaranta) wskazanym w ust. 2 niniejszego paragrafu umowy oraz stan plomb i innych umieszczonych na nim zabezpieczeń, o ile takie zabezpieczenia zostały zastosowane.
	2. Wykonawca w chwili wykonania w całości przedmiotu niniejszej umowy, wyda Zamawiającemu dokument gwarancyjny (oświadczenie gwaranta) oraz karty gwarancyjne producentów odpowiadające treści umowy którego treść będzie obejmowała co najmniej następujące informacje: nazwę i adres gwaranta lub jego przedstawiciela w Rzeczypospolitej Polskiej, czas trwania i terytorialny zasięg ochrony gwarancyjnej, uprawnienia przysługujące Zamawiającemu w razie stwierdzenia wady fizycznej, a także stwierdzenie, że gwarancja nie wyłącza, nie ogranicza ani nie zawiesza uprawnień Zamawiającego wynikających z przepisów o rękojmi za wady przedmiotu umowy. Dostarczenie przez Wykonawcę oświadczeń gwarancyjnych złożonych przez producentów nie zwalnia Wykonawcy z obowiązków gwarancyjnych lub spełnienia innych obowiązków wynikających z niniejszej Umowy.
	3. W przypadku stwierdzenia wad w wykonanym przedmiocie umowy Wykonawca zobowiązuje się do jego nieodpłatnej wymiany lub usunięcia wad na zasadach i w trybie określonym w treści dokumentu gwarancyjnego (oświadczenie gwaranta) wskazanego w ust. 2 powyżej, z uwzględnieniem dalszych postanowień niniejszego paragrafu umowy.
	4. Wykonawca udziela gwarancji na okres **36 miesięcy** na dostarczony przedmiot umowy (licząc od dnia następnego po dniu wykonania przedmiotu umowy – tj. po dacie odbioru końcowego przedmiotu umowy), z uwzględnieniem zapisów dotyczących warunków gwarancyjnych wynikających z SWZ.
	5. Uprawnienia Zamawiającego z tytułu gwarancji i rękojmi za wady będą realizowane przez producenta lub autoryzowany przez niego serwis lub osoby na koszt Wykonawcy na zasadach określonych w treści SWZ, przy czym wszelkie działania organizacyjne i koszty związane ze świadczeniem usługi gwarancyjnej poza miejscem wykonania umowy ponosi Wykonawca.
	6. Czas reakcji na zgłoszone wady (przystąpienie do niezwłocznego usunięcia wady przez stawiennictwo serwisanta) w ciągu 48 godzin od zgłoszenia wady (powiadomienia faksowego lub e-mailowego), z wyłączeniem dni ustawowo wolnych od pracy.
	7. Naprawa gwarancyjna będzie wykonana w terminie nie dłuższym niż 7 dni od zgłoszenia (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy), licząc od dnia przyjęcia zgłoszenia przez serwis (faxem lub e-mailem). W przypadku konieczności sprowadzenia specjalistycznych części zamiennych, termin ten nie może być dłuższy niż 21 dni roboczych (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy), chyba, że Strony uzgodnią inny termin co zostanie potwierdzone pisemnym protokołem konieczności.
	8. W ramach gwarancji Wykonawca będzie zobowiązany m.in. do nieodpłatnej (wliczonej w cenę oferty) bieżącej konserwacji, serwisu i przeglądów technicznych wynikających z warunków gwarancji i naprawy przedmiotu umowy w okresie gwarancyjnym. Wykonawca udziela gwarancji na wszystkie części składowe, podzespoły, oraz inne elementy wchodzące w skład przedmiotu umowy lub usługi nabyte u podmiotów trzecich przez Wykonawcę. Gwarancji podlegają usterki, wady materiałowe i konstrukcyjne, a także nie spełnianie funkcji użytkowych przez dostarczony sprzęt, deklarowanych przez Wykonawcę. Wszystkie koszty związane z realizacją gwarancji pokrywa Wykonawca.
	9. Wykonawca jest zobowiązany do świadczenia w okresie gwarancji konserwacji (w ramach której Wykonawca dostarcza również na swój koszt materiały niezbędne do wykonania konserwacji) i przeglądów przedmiotu umowy wynikających z treści gwarancji producenta/ów. Dodatkowo, po każdym roku eksploatacji, przy czym ostatnie z nich muszą być przeprowadzone na dwa miesiące przed końcem okresu gwarancji udzielonej przez Wykonawcę, Wykonawca zobowiązany jest wykonać bezpłatny przegląd gwarancyjny wszystkich urządzeń i elementów. Po wykonaniu przeglądu, Wykonawca jest zobowiązany do przekazania Zamawiającemu raportu przeglądu.
	10. Wykonawca gwarantuje najwyższą jakość dostarczonego przedmiotu umowy zgodnie ze specyfikacją techniczną. Odpowiedzialność z tytułu gwarancji obejmuje zarówno wady powstałe z przyczyn tkwiących w przedmiocie umowy w chwili dokonania odbioru przez Zamawiającego jak i wszelkie inne wady fizyczne, powstałe z przyczyn, za które Wykonawca ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
	11. Bieg terminu gwarancji rozpoczyna się w dniu następnym, po odbiorze przedmiotu umowy, przy czym w przypadku wymiany wadliwego elementu przedmiotu umowy na nowy, termin gwarancji dla tego elementu biegnie na nowo od chwili dostarczenia Zamawiającemu nowego urządzenia.
	12. Okres gwarancji ulega automatycznie przedłużeniu o okres naprawy, tj. czas liczony od zgłoszenia do usunięcia awarii lub wady.
	13. W przypadku, gdy Wykonawca nie wypełni warunków gwarancji lub nie zastosuje się do powyższych zasad, Zamawiający jest uprawniony do usunięcia wad w drodze naprawy, na ryzyko i koszt Wykonawcy, zachowując przy tym inne uprawnienia przysługujące mu na podstawie umowy. W takich przypadkach Zamawiający ma prawo zaangażować inny podmiot do usunięcia wad, a Wykonawca zobowiązany jest pokryć związane z tym koszty w ciągu 14 dni od daty otrzymania wezwania wraz z dowodem zapłaty.
	14. Zamawiający może wykonywać uprawnienia z tytułu rękojmi za wady fizyczne rzeczy niezależnie od uprawnień wynikających z gwarancji i jest on uprawniony do żądania jej demontażu i ponownego zamontowania po dokonaniu wymiany na wolną od wad lub usunięciu wady. Do odpowiedzialności Wykonawcy za wady prawne przedmiotu umowy stosuje się przepisy kodeksu cywilnego.
	15. Uprawnienia z tytułu rękojmi za wady fizyczne wygasają po upływie okresu 24 miesięcy, licząc od momentu dostarczenia Zamawiającemu przedmiotu umowy w całości potwierdzonego podpisanym protokołem odbioru bez zastrzeżeń, przy czym w razie wykonywania przez Zamawiającego uprawnień z gwarancji bieg terminu do wykonania uprawnień z tytułu rękojmi ulega zawieszeniu z dniem zawiadomienia Wykonawcy o wadzie. Termin ten biegnie dalej od dnia odmowy przez Wykonawcę wykonania obowiązków wynikających z gwarancji albo bezskutecznego upływu terminu określonego na usunięcie wady przedmiotu umowy.
	16. Zamawiający zobowiązuje się dotrzymywać podstawowych zasad eksploatacji określonych przez producenta w treści oświadczenia gwaranta zawartego w dokumentach gwarancyjnych lub instrukcjach eksploatacji dostarczonych przez Wykonawcę, w zakresie w jakim nie jest ono sprzeczne z postanowieniami niniejszego paragrafu umowy.

§ 8

* + 1. Wykonawca odpowiada z tytułu rękojmi za wady przedmiotu umowy, które ujawnią się w terminie 24 miesięcy liczonych od dnia zakończenia realizacji przedmiotu umowy potwierdzonego odbiorem końcowym.
		2. W razie stwierdzenia wad przedmiotu umowy lub jego części Zamawiający może żądać ich usunięcia w wyznaczonym stosownym terminie, nie dłuższym niż 14 dni. W przypadku konieczności sprowadzenia przez Wykonawcę specjalistycznych części zamiennych termin może zostać wydłużony do 30 dni lub o inny odpowiednio umotywowany.
		3. Uprawnienia Zamawiającego z tytułu rękojmi za wady przedmiotu umowy w postaci roszczenia o usunięcie wady przedmiotu umowy, przedawniają się z upływem roku od chwili:
	1. kiedy Zamawiający stwierdził istnienie tej wady przedmiotu umowy,
	2. powzięcia przez Zamawiającego informacji o istnieniu tej wady prawnej lub z momentem uprawomocnienia się orzeczenia sądu. Ten sam termin przedawnienia stosuje się w razie złożenia przez Zamawiającego oświadczenia o obniżeniu wynagrodzenia albo odstąpienia od umowy.
		1. W razie, gdy Wykonawca nie spełnił roszczenia o usunięcie wady przedmiotu umowy, bieg rocznego terminu do złożenia oświadczeń o obniżenie wynagrodzenia albo odstąpienia od umowy przez Zamawiającego rozpoczyna się z chwilą bezskutecznego upływu terminu do zaspokojenia przedmiotowych roszczeń.
		2. Uprawnienia te nie wygasają w terminie wskazanym w ust. 4, jeśli Wykonawca podstępnie zataił przed Zamawiającym wadę przedmiotu umowy.
		3. Bieg rocznego terminu przedawnienia do wykonywania uprawnień z tytułu rękojmi za wady przedmiotu umowy ulega zawieszeniu w przypadku:
	3. dochodzenia przez Zamawiającego przed sądem albo sądem polubownym jednego z uprawnień z tytułu rękojmi za wady, termin do wykonania innych uprawnień, przysługujących mu z tego tytułu, ulega zawieszeniu do czasu prawomocnego zakończenia postępowania;
	4. dochodzenia przez Zamawiającego w postępowaniu mediacyjnym jednego z uprawnień z tytułu rękojmi za wady, termin do wykonania innych uprawnień, przysługujących mu z tego tytułu, ulega zawieszeniu do dnia odmowy przez sąd zatwierdzenia ugody zawartej przed mediatorem lub bezskutecznego zakończenia mediacji.
		1. Wykonawca odpowiada za wady przedmiotu umowy tkwiące w nim w dniu odbioru danej części przedmiotu umowy, potwierdzonego podpisanymi przez przedstawicieli Stron umowy protokołem odbioru.
		2. W razie istnienia wady przedmiotu umowy w terminie określonym w ust. 1 niniejszego paragrafu umowy, Zamawiającemu wobec Wykonawcy przysługuje:
		3. złożenie pisemnego oświadczenia o obniżeniu wynagrodzenia brutto wskazanego w § 4 ust. 2 umowy w proporcji do ww. wynagrodzenia, w jakiej wartość wadliwej części przedmiotu umowy pozostaje do danej części przedmiotu umowy nie obarczonego wadą, chyba, że Wykonawca bez zbędnej zwłoki nieprzekraczającej 7 dni roboczych (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy) i utrudnień dla Zamawiającego dostarczy mu daną część przedmiotu umowy wolną od wady lub tą wadę usunie. Jednakże oświadczenie Zamawiającego jest wiążące dla Wykonawcy, o ile wada danej części przedmiotu umowy była już usuwana lub została dostarczona niewadliwa dana część przedmiotu umowy, a także, gdy Wykonawca nie zadośćuczynił żądaniu Zamawiającego dostarczenia mu danej części przedmiotu wolnej od wady lub usunięcia tej wady w ww. terminie,
		4. złożenie pisemnego oświadczenia o odstąpieniu od niniejszej umowy z powodu istotnej wady danej części przedmiotu umowy uniemożliwiającej Zamawiającego realizację przedmiotu zamówienia publicznego będącego przedmiotem umowy, chyba, że Wykonawca bez zbędnej zwłoki nieprzekraczającej 7 dni roboczych (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy) i utrudnień dla Zamawiającego dostarczy mu daną część przedmiotu umowy wolną od wady lub tą wadę usunie. Jednakże oświadczenie Zamawiającego jest wiążące dla Wykonawcy, o ile wada danej części przedmiotu umowy była już usuwana lub została dostarczona niewadliwa dana część przedmiotu umowy, a także, gdy Wykonawca nie zadośćuczynił żądaniu Zamawiającego dostarczenia mu danej części przedmiotu wolnej od wady lub usunięcia tej wady w ww. terminie,
		5. roszczenie o usunięcie wady bez zbędnej zwłoki nieprzekraczającej 7 dni roboczych (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy) i utrudnień dla Zamawiającego, chyba, że zadośćuczynienie przedmiotowemu roszczeniu przez Wykonawcę okaże się niemożliwym lub wiąże się ono z nadmiernymi kosztami po stronie Wykonawcy w stosunku do możliwości dostarczenia danej części przedmiotu umowy wolnego od niniejszej wady, w szczególności usunięcie wady przedmiotu umowy przewyższa wysokość wynagrodzenia brutto wskazanego w § 4 ust. 2 umowy.
1. Wykonawca jest zobowiązany przyjąć od Zamawiającego wadliwy przedmiot umowy.
2. Jeżeli Zamawiający uniknął utraty w całości lub w części przedmiotu umowy albo skutków jego obciążenia na korzyść osoby trzeciej, Wykonawca będzie wolny od odpowiedzialności z tytułu rękojmi za wady prawne, z chwilą zwrotu Zamawiającemu zapłaconej wcześniej przez niego sumy lub wartości spełnionego świadczenia wraz z odsetkami i kosztami na rzecz osoby trzeciej.
3. Jeżeli z powodu wady prawnej przedmiotu umowy Zamawiający był zobowiązany wydać je osobie trzeciej Wykonawca zwróci Zamawiającemu odpowiednią część wynagrodzenia brutto wskazanego w § 4 ust. 2 umowy stanowiącego wartość wadliwego przedmiotu umowy.
4. Niezależnie od uprawnień Zamawiającego wynikających z powyższych zapisów niniejszego paragrafu umowy:
	* 1. w przypadku wad, niezależnie od uprawnień Zamawiającego do złożenia oświadczenia o obniżeniu wynagrodzenia albo odstąpieniu od umowy, Zamawiający będzie domagał się od Wykonawcy odszkodowania za zawarcie umowy nie wiedząc, że jej przedmiot był obarczony wadą, choćby szkoda była następstwem okoliczności, za które Wykonawca nie ponosi odpowiedzialności. Przedmiotowe odszkodowanie obejmuje w szczególności zwrot kosztów zawarcia umowy, kosztów odebrania, przewozu, przechowania wadliwego przedmiotu umowy i jego ubezpieczenia, zwrot dokonanych nakładów w takim zakresie, w jakim Zamawiający nie odniósł korzyści z tych nakładów. Tożsame uprawnienie przysługuje Zamawiającemu również w przypadku dochodzenia przez niego roszczeń o dostarczenie rzeczy wolnej od wad albo o usunięcie wady przedmiotu umowy. Nie uchybia to przepisom o obowiązku naprawienia szkody na zasadach ogólnych,
		2. w przypadku wad prawnych, niezależnie od uprawnień Zamawiającego do złożenia oświadczenia o obniżeniu wynagrodzenia albo odstąpieniu od umowy, Zamawiający będzie domagał się od Wykonawcy odszkodowania za zawarcie umowy nie wiedząc, że jej przedmiot był obarczony wadą prawną, choćby szkoda była następstwem okoliczności, za które Wykonawca nie ponosi odpowiedzialności. Przedmiotowe odszkodowanie obejmuje w szczególności zwrot kosztów zawarcia umowy, kosztów odebrania, przewozu, przechowania wadliwego przedmiotu umowy i jego ubezpieczenia, zwrot dokonanych nakładów w takim zakresie, w jakim Zamawiający nie odniósł z niego korzyści, a nie otrzymał ich zwrotu od osoby trzeciej, oraz zwrotu kosztów procesu. Tożsame uprawnienie przysługuje Zamawiającemu również w przypadku dochodzenia przez niego roszczeń o usunięcie wady przedmiotu umowy. Nie uchybia to przepisom o obowiązku naprawienia szkody na zasadach ogólnych.

§ 9

* 1. Niezależnie od przypadków uregulowanych w Kodeksie cywilnym, Stronom przysługuje prawo odstąpienia od niniejszej umowy w razie zaistnienia okoliczności w niej wskazanych.
	2. Zamawiający może odstąpić od umowy, nie wcześniej niż w terminie 7 (siedmiu) dni i nie później niż w terminie 30 dni od dnia powzięcia informacji o tym, że :
		1. Wykonawca na skutek swojej niewypłacalności nie wykonuje zobowiązań pieniężnych przez okres co najmniej 3 miesięcy,
		2. została podjęta likwidacja Wykonawcy lub rozwiązanie Wykonawcy bez przeprowadzenia likwidacji, bądź nastąpi zakończenie prowadzenia działalności gospodarczej przez Wykonawcę bądź wykreślenie Wykonawcy jako przedsiębiorcy z CEIDG albo śmierci Wykonawcy będącego osobą fizyczną,
		3. Wykonawca bez uzasadnionego powodu nie rozpoczął realizacji przedmiotu umowy lub w przypadku wstrzymania prac przez Zamawiającego, nie podjął ich w ciągu 3 dni roboczych od chwili otrzymania decyzji o podjęciu realizacji od Zamawiającego za pomocą e-maila pod adres …………@………….,
		4. Wystąpiły u Wykonawcy duże trudności finansowe, w szczególności zajęcia komornicze lub inne zajęcia uprawnionych organów o łącznej wartości przekraczającej 200 000,00 PLN (słownie: dwieście tysięcy złotych),
		5. Wykonawca dostarczył sprzęt lub realizuje usługi nieodpowiadające treści umowy;
	3. Ponadto Zamawiający może odstąpić od umowy, w przypadku gdy zwłoka Wykonawcy w wykonaniu przedmiotu umowy przekroczyła 30 dni i pomimo wyznaczenia dodatkowego 14dniowego terminu Wykonawca nie wykonał przedmiotu umowy zgodnie z treścią umowy.
	4. Ponadto w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach (art. 456 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych). W takim przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części przedmiotu umowy.
	5. Zamawiający może rozwiązać umowę w trybie natychmiastowym, w przypadku, gdy:
	6. Wykonawca w chwili zawarcia niniejszej umowy podlegał wykluczeniu na podstawie art. 108 ust. 1 ustawy PZP,
	7. Zamawiający udzielił Wykonawcy niniejszego zamówienia publicznego na podstawie przepisów krajowych, które zostały uznane przez Trybunał Sprawiedliwości UE, w ramach procedury przewidzianej w art. 258 Traktatu o Funkcjonowaniu UE, że Rzeczpospolita Polska uchybiła zobowiązaniom wynikających z Traktatów lub Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE (Dz. Urz. UE L 2014 Nr 94 str. 65 ze zm.).
	8. Wykonawcy nie przysługuje odszkodowanie z tytułu odstąpienia przez Zamawiającego od umowy z powodu okoliczności leżących po stronie Wykonawcy albo w razie rozwiązania umowy na podstawie ust. 4 niniejszego paragrafu umowy.
	9. Zamawiając, korzystając z umownego lub ustawowego prawa odstąpienia od umowy może odstąpić – zgodnie ze swoim wyborem – od całości umowy lub od jej części.
	10. Odstąpienie od umowy albo rozwiązanie niniejszej umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.
	11. Odstąpienie od umowy albo rozwiązania niniejszej umowy nie wpływa na istnienie i skuteczność roszczeń o zapłatę kar umownych.

§ 10

* + 1. Strony zastrzegają sobie prawo do naliczania i dochodzenia kar umownych za niezgodne z niniejszą umową lub nienależyte wykonanie zobowiązań wynikających z umowy.
		2. Wykonawca, za wyjątkiem, gdy postawę naliczenia kar umownych stanowią jego zachowania niezwiązane bezpośrednio lub pośrednio z przedmiotem umowy lub jej prawidłowym wykonaniem, zapłaci Zamawiającemu karę umowną w następujących przypadkach:
	1. odstąpienia od umowy wskutek okoliczności niezależnych od Zamawiającego - w wysokości 20% wynagrodzenia netto ustalonego w § 4 ust. 2 umowy;
	2. niewykonania lub nienależytego wykonania umowy - w wysokości 20% wynagrodzenia netto ustalonego w § 4 ust. 2 umowy, przy czym nienależyte wykonanie umowy to wykonanie w sposób sprzeczny z treścią umowy lub ofertą Wykonawcy lub treścią SWZ, jak również niezapewniające osiągnięcia wymaganych parametrów, funkcjonalności i zakresów wynikających z SWZ wraz z załącznikami oraz parametrów użytkowych przedmiotu umowy;
	3. zwłoki w wykonaniu przedmiotu umowy - w wysokości 0,1% wynagrodzenia netto ustalonego w § 4 ust. 2 umowy za każdy dzień zwłoki, licząc od dnia wykonania przedmiotu umowy, określonego w § 1 ust. 6 umowy – w wysokości nie wyższej niż 20% wynagrodzenia brutto ustalonego w § 4 ust. 2 umowy;
	4. zwłoki w usunięciu wad przedmiotu umowy stwierdzonych przy odbiorze - w wysokości 0,1% wynagrodzenia netto ustalonego w § 4 ust. 2 umowy za każdy dzień zwłoki, licząc od następnego dnia po upływie terminu określonego przez Zamawiającego na usunięcie wad - w wysokości nie wyższej niż 20% wynagrodzenia brutto ustalonego w § 4 ust. 2 umowy;
	5. zwłoki w usunięciu wad stwierdzonych w okresie gwarancji lub rękojmi w wysokości 0,1% wynagrodzenia netto ustalonego w § 4 ust. 2 umowy za każdy dzień zwłoki, licząc od dnia następnego po upływie terminu (dnia) ustalonego zgodnie z treścią odpowiednio § 7 lub § 8 umowy albo w pisemnym oświadczeniu Stron w formie protokołu konieczności, nie więcej niż 20% wynagrodzenia brutto ustalonego w § 4 ust.2 umowy.
	6. zwłoki w doręczeniu korekty faktury, w terminie określonym w § 4 ust. 5 uwzgledniającej w odrębnej pozycji należność z tytułu podatku VAT - w wysokości stanowiącej równowartość należnego podatku od towarów i usług VAT z tytułu przedmiotowej dostawy sprzętu komputerowego (komputerowego zestawu roboczego) objętego zastosowaniem stawki 0% VAT.
	7. nieprzeprowadzenie szkolenia dla pracowników Zamawiającego - w wysokości 10 000,00 PLN (słownie: dziesięć tysięcy złotych 00/100) za każde ww. uchybienie Wykonawcy.
1. Wykonawca ma prawo do żądania zapłaty kary umownej w przypadku odstąpienia od umowy przez Wykonawcę z wyłącznej winy Zamawiającego - w wysokości 10% wynagrodzenia netto ustalonego w § 4 ust. 2 umowy.
2. Strony mogą dochodzić na zasadach ogólnych odszkodowania przewyższającego wysokość zastrzeżonych kar umownych.
3. Strony mogą dochodzić na zasadach ogólnych odszkodowania przewyższającego wysokość zastrzeżonych kar umownych, przy czym kary umowne mają charakter zaliczalny na poczet przedmiotowego odszkodowania uzupełniającego dochodzonego przez daną Stronę umowy.
4. Zapisy umowy dotyczące naliczania kar umownych nie mają zastosowania za zachowanie Wykonawcy niezwiązane bezpośrednio lub pośrednio z przedmiotem umowy lub jej prawidłowym wykonaniem. Wykonawca nie ponosi odpowiedzialności za okoliczności, za które wyłączną odpowiedzialność ponosi zamawiający.
5. Roszczenie o zapłatę kary umownej staje się wymagalne w dniu następnym po dniu wystąpienia okoliczności uzasadniającej powstanie zobowiązania do zapłaty kary umownej z określonego tytułu.
6. Strony dopuszczają kumulację kar umownych , o których mowa w niemniejszym paragrafie umowy, przy czym łączna wysokość kar umownych nie może przekroczyć 30% Wynagrodzenia netto, o którym mowa w § 4 ust. 2.
7. Roszczenie o zapłatę kar umownych staje się wymagalne począwszy od dnia następnego po dniu, w którym miały miejsce okoliczności faktyczne określone w niniejszej umowie stanowiące podstawę do ich naliczenia.
8. Zamawiający jest uprawniony do potrącenia ewentualnych kar umownych z należnej Wykonawcy kwoty wynagrodzenia określonej w fakturze lub innych ewentualnych wierzytelności Wykonawcy względem Zamawiającego.
9. Zapłata kar umownych nie zwalnia Wykonawcy od obowiązku wykonania umowy.
10. W przypadku odstąpienia lub wypowiedzenia umowy, Strony zachowują prawo egzekucji kar umownych.

§ 11

* + - 1. Przez okoliczności siły wyższej strony rozumieją zdarzenie zewnętrzne o charakterze nadzwyczajnym, którego nie można było przewidzieć ani jemu zapobiec, w szczególności takie jak: wojna, stan wyjątkowy, powódź, pożar, epidemia choroby zakaźnej czy też zasadnicza zmiana sytuacji społeczno – gospodarczej.
			2. Jeżeli wskutek okoliczności siły wyższej Strona nie będzie mogła wykonywać swoich obowiązków umownych w całości lub w części, niezwłocznie powiadomi o tym drugą stronę. W takim przypadku Strony uzgodnią sposób i zasady dalszego wykonywania umowy lub umowa zostanie rozwiązana.
			3. Bieg terminów określonych w niniejszej umowie ulega zawieszeniu przez czas trwania przeszkody spowodowanej siłą wyższą.

§ 12

* + - * 1. Wszelkie oświadczenia Stron skutkujące zmianą lub wygaśnięciem Umowy będą składane na piśmie pod rygorem nieważności listem poleconym lub za potwierdzeniem ich złożenia.
				2. Ewentualna nieważność jednego lub kilku postanowień niniejszej Umowy nie wpływa na ważność Umowy w całości. W takim przypadku Strony zastępują nieważne postanowienie postanowieniem zgodnym z celem i innymi postanowieniami Umowy.
				3. W razie rozbieżności pomiędzy treścią SWZ a postanowieniami umowy oraz w sprawach nieuregulowanych niniejszą umową priorytet nadaje się zapisom SWZ i jej załącznikom.

§ 13

1. Strony dopuszczają możliwość zmiany Umowy po uprzednim sporządzeniu protokołu konieczności, przy zachowaniu ryczałtowego charakteru ceny Umowy, poprzez podpisanie aneksu do Umowy, w następujących przypadkach:
	1. zmiany terminu realizacji przedmiotu umowy, w tym dostawy lub usług towarzyszących (początkowego, końcowego) poprzez jego skrócenie lub przedłużenie i/lub zmiany sposobu realizacji poprzez wprowadzenie etapów realizacji, zawieszenia realizacji - ze względu na przyczyny leżące po stronie Zamawiającego, dotyczące w szczególności braku przygotowania/przekazania miejsca realizacji/dostawy, nieobecność pracownika odpowiedzianego za realizację lub odbiór przedmiotu umowy, lub przyczyny leżące po stronie producenta sprzętu dotyczące udokumentowanych problemów związanych z produkcją lub dostawą sprzętu lub z innych przyczyn niezależnych od Stron spowodowanych przez siłę wyższą,
	2. wydłużenia terminu gwarancji, w sytuacji przedłużenia jej przez producenta/Wykonawcę,
	3. zmiany określonego typu, modelu, nazwy, producenta przedmiotu umowy bądź jego elementów, poprawy jakości lub innych parametrów charakterystycznych dla danego elementu dostawy lub zmiany technologii na równoważną lub lepszą w szczególności w przypadku zakończenia jego produkcji lub wstrzymania lub wycofania go z produkcji po przedstawianiu stosownych dokumentów od producenta lub dystrybutora, z tym że cena wskazana w §4 nie może ulec podwyższeniu, a parametry techniczne nie mogą być gorsze niż wskazane w treści oferty,
	4. aktualizacji rozwiązań z uwagi na postęp technologiczny lub zmiany obowiązujących przepisów
		1. Ponadto dopuszcza się zastąpienie dotychczasowego Wykonawcy niniejszej umowy przez inny podmiot spełniający warunki udziału w postępowaniu oraz niepodlegający wykluczeniu z postępowania na mocy art. 108 ust. 1 i art. 109 ust. 1 ustawy PZP, w razie gdy nastąpiło połączenie, podział, przekształcenie, upadłość, restrukturyzacja, nabycie dotychczasowego Wykonawcy lub nabycie jego przedsiębiorstwa przez ww. podmiot.
		2. Strony umowy mogą dokonywać zmian umowy, które nie są istotne w rozumieniu art. 454 ust. 2 ustawy PZP, poprzez zawarcie pisemnego aneksu pod rygorem nieważności.
		3. Zmiany nie dotyczące postanowień umownych np. gdy z przyczyn organizacyjnych konieczna będzie zmiana danych teleadresowych określonych w umowie, gdy zmianie ulegnie numer konta bankowego jednej ze Stron nastąpią poprzez przekazanie pisemnego oświadczenie Strony, której te zmiany dotyczą, drugiej Stronie

§ 14

Strony ustalają, że do bezpośrednich kontaktów w trakcie wykonywania niniejszej Umowy, mających na celu sprawną realizację zamówienia i jego bieżący nadzór oraz weryfikację i kontrolę prawidłowości powołane zostają następujące osoby:

* 1. ze Strony Zamawiającego –

……………………… tel.: …………., e-mail: ………………….;

* 1. ze Strony Wykonawcy –

……………………… tel.: …………., e-mail: …………………..

1. Osoby wymienione w ust. 1. nie są upoważnione do podejmowania decyzji powodujących zmianę warunków umowy, w szczególności wzrostu kosztów, zwiększenia lub zmiany zakresu przedmiotu umowy.
2. Zamawiający może w trakcie realizacji przedmiotu umowy zgłosić uzasadniony sprzeciw wobec osoby wymienionej w ust. 1.2. W takim przypadku Wykonawca jest zobowiązany do jej zmiany w terminie 7 dni od zgłoszenia przez Zamawiającego.
3. Strony zgodnie ustalają, że zmiana osób wykazanych w ust. 1 oraz przeznaczonych zgodnie z ofertą do realizacji umowy w treści oferty Wykonawcy wymaga uprzedniej pisemnej zgody Zamawiającego i dopuszczalna jest wyłącznie w wyjątkowych sytuacjach, w szczególności z powodu choroby lub innych zdarzeń losowych powodujących niemożność wykonywania powierzonego jej zakresu obowiązków, a wskazane w zastępstwie osoba lub osoby muszą posiadać kwalifikacje niemniejsze niż jej poprzednik.
4. W przypadku zmiany przedstawiciela przez jedną ze stron zobowiązana jest ona powiadomić o tym na piśmie drugą stronę w terminie 3 dni.
5. Zmiana osób wymieniowych w ust. 1 nie stanowi zmiany umowy.

§ 15

Wszelkie oświadczenia Stron umowy będą składane na piśmie pod rygorem nieważności, listem poleconym lub za potwierdzeniem ich złożenia, chyba że wyraźne postanowienie niniejszej umowy przewiduje inny sposób złożenia oświadczenia.

Wszelkie zmiany, w tym uzupełnienia niniejszej umowy, rozwiązanie lub odstąpienie od umowy wymagają formy pisemnej pod rygorem nieważności.

Żadna ze Stron nie jest uprawniona do przeniesienia swoich praw i zobowiązań z niniejszej umowy bez uzyskania pisemnej zgody drugiej Strony, pod rygorem nieważności, w szczególności Wykonawcy nie przysługuje prawo przenoszenia wierzytelności wynikających z niniejszej umowy na osoby trzecie bez uprzedniej pisemnej zgody Zamawiającego.

Strony zobowiązują się do każdorazowego powiadamiania się listem poleconym o zmianie adresu swojej siedziby, pod rygorem uznania za skutecznie doręczoną korespondencję wysłaną pod dotychczas znany adres.

Strony ustalają, iż pod pojęciem dni roboczych rozumieją dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy .

Wszelkie spory wynikające z niniejszej umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.

W sprawach nieunormowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t. j. Dz. U. 2020 poz. 1740 z późn. zm.), ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t. j. Dz. U. 2021 poz. 1129 z późn. zm.), ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (t. j. Dz. U. 2020 poz. 1333 z późn. zm.) oraz ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. 2020 poz. 1842 z późn. zm.) wraz z przepisami wykonawczymi.

§ 16

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Strony zgodnie oświadczają, że z uwagi na fakt zawarcia niniejszej umowy w formie elektronicznej za pomocą kwalifikowanego podpisu elektronicznego powstały w ten sposób dokument elektroniczny stanowi poświadczenie, iż Strony zgodnie złożyły oświadczenia woli w nim zawarte, zaś datą zawarcia jest dzień złożenia ostatniego (późniejszego) oświadczenia woli o jej zawarciu przez umocowanych przedstawicieli każdej ze Stron.

Załącznik do umowy:

nr 1 – lista podwykonawców z określeniem zakresu i wartości robót przewidzianych do wykonania, o ile są przewidziani na etapie zawarcia umowy.

**……………………………… ………………………………**

**Zamawiający Wykonawca**

**Załącznik A do SWZ**

**Przetarg nieograniczony na modernizację infrastruktury sieciowej Wydziału Biochemii, Biofizyki i Biotechnologii Uniwersytetu Jagiellońskiego**

1. **Opis ogólny przedmiotu zamówienia**

Zamawiający planuję modernizację aktualnie posiadanej infrastruktury sieciowej przewodowej oraz bezprzewodowej na obiekcie Wydziału Biochemii, Biofizyki i Biotechnologii UJ znajdującym się na ulicy Gronostajowej 7 w Krakowie.

Aktualna infrastruktura składa się Centralnego Punktu Dystrybucyjnego „Serwerownia” połączonych za pomocą sieci światłowodowej OM4 z dziewięcioma piętrowymi punktami dystrybucyjnymi: „IDF A”, „IDF B”, „IDF C”, „IDF D”, „IDF E”, „IDF NMR”, „IDF Bioinformatycy”, „IDF Szatnia”, „IDF Trójkąt”. W ramach niniejszego postępowania konieczne będzie zbudowanie i podłączenie oraz wyposażenie w niezbędne akcesoria trzech nowych punktów dystrybucyjnych: „IDF Sekretariat”, „IDF Horyzont”, „IDF Dydaktyka” oraz wykoananie nowego połączenia za pomocą światłowodu punktów „IDF B” z „IDF Bioinformatycy”.

* Nowy punkt „IDF Horizon” będzie trzeba utworzyć i wyposażyć w niezbędne akcesoria w tym stojącą szafę RACK 19’’ o wysokości min. 42U, i połączyć z „IDF Serwerownia” przy pomocy światłowodu.
* Nowy punkt „IDF Sekretariat” będzie trzeba utworzyć i wyposażyć w niezbędne akcesoria w tym wiszącą szafę RACK 19’’ o wysokości min. 12U oraz rozprowadzić z punktu „IDF Sekretariat” 48 nowych miedzianych przyłączeń strukturalnych kat. min. 6a (Ethernet) wraz z montażem odpowiedniego patchpanela zakończonego złączami RJ45 po stronie punktu dystrybucyjnego oraz 24 podwójnymi gniazdami RJ45 po stronie stanowisk klienckich przy założeniu że żaden tor nie przekracza 100m.
* Nowy punkt „IDF Dydaktyka” będzie trzeba utworzyć i wyposażyć w niezbędne akcesoria w tym w wiszącą szafę RACK 19’’ o wysokości min. 12U.
* Istniejący punkty „IDF B” oraz „IDF Bioinformatycy” należy połączyć za pomocą światłowodu i wyposażyć w niezbędne akcesoria.

Powyższe nowe punkty dostępowe oraz relację „IDF B” – „IDF Bioinformatycy” należy połączyć przy pomocy 24 żyłowego światłowodu. Dla powyżej wymienionych nowo tworzonych relacji światłowodowych będzie należało zamontować po dwie krosownice (po jednej na stronę) oraz wykonać spaw światłowodu dla 24 włókien z każdej strony i wyposażyć w adaptery MM typu LC/LC duplex OM4. Projektowany kabel światłowodowy musi posiadać wielomodowe włókna 50/125 μm, charakteryzować się niskim pikiem wodnym (ang. low water peak fiber) i wydajnością transmisyjną OM4.

Każdy piętrowy punkt dystrybucyjny obsługuje okablowanie strukturalne kat. min. 5e, które zakończone jest panelami RJ45 zainstalowanymi w szafie Rack 19”. Przewidujemy obsługę wszystkich zakończonych łączy RJ45 w każdym z punktów dystrybucyjnych przez nowo zamawiane urządzenia aktywne z prędkością min. 1 Gigabit Ethernet wyposażone w możliwość zasilania poprzez skrętkę PoE+ zgodnie ze standardem min. IEEE 802.3at (30W per port). Część punktów dystrybucyjnych („IDF A”, „IDF B”, „IDF C”, „IDF NMR”, „IDF Bioinformatycy”, „IDF E” oraz „IDF Horizon”) musi być wyposażona w dodatkowe urządzenie lub urządzenia zapewniające obsługę min. 12 portów 10 Gigabit Ethernet na skrętkę 1/2.5/5/10GBase-T oraz min. 12 portów 1/10 Gigabit Ethernet na interfejsy światłowodowe SFP+. Przełączniki te będą przeznaczone dla wymagających urządzeń, aparatury pomiarowej, lokalnych serwerów grupy roboczej lub wymagających użytkowników. Urządzenia aktywne obsługujące piętrowe punkty dystrybucyjne muszą być dołączone do szkieletu sieci z zapewnieniem odporności na awarię pojedynczego urządzenia brzegowego, pojedynczego łącza światłowodowe lub pojedynczej wkładki światłowodowej. Przepustowość urządzeń aktywnych umieszczonych w piętrowych punktach dystrybucyjnych i obsługujących porty Gigabit Ethernet musi wynosić minimum 2 x 10Gb/s. Przełączniki w poszczególnych punktach dystrybucyjnych powinny być połączone w stosy, aby zminimalizować liczbę zarządzanych urządzeń oraz liczbę niezbędnych łączy światłowodowych do Centralnego Punktu Dystrybucyjnego. Maksymalna liczba urządzeń w projektowanym stosie nie może przekraczać 4 urządzeń i 192 portów 10/100/1000Base-T. W przypadku wymaganej większej liczby obsługiwanych portów w piętrowym punkcie dystrybucyjnym konieczne będzie zbudowanie dodatkowego stosu i każdy ze stosów musi być połączony z Centralnym Punktem Dystrybucyjnym osobnymi odpornymi na awarie łączami. Jeśli piętrowy punkt dystrybucyjny wyposażony jest w przełącznik lub stos przełączników obsługujących porty o przepustowości większej niż 1 Gigabit Ethernet to połączenie tego urządzenia do Centralnego Punktu Dystrybucyjnego musi się odbywać za pomocą odpornych na awarie min. 2 połączeń o przepustowości większej niż 10 Gigabit Ethernet np. 25G, 40G lub 100G.

Centralny Punkt Dystrybucyjny musi być wyposażony w min. dwa przełączniki szkieletowe umożliwiające agregację wszystkich łączy 10 Gigabit Ethernet oraz 25G, 40G lub 100G przychodzących z piętrowych punktów dystrybucyjnych. Połączenie pomiędzy przełącznikami szkieletowymi musi być zrealizowane z wykorzystaniem min. 2 łączy 100 Gigabit Ethernet. Należy przewidzieć w obydwu przełącznikach szkieletowych dodatkowe min. 2 porty QSFP28, które mogą pracować z prędkością 40 lub 100 Gb/s, do podłączenia sieci LAN do reszty infrastruktury sieciowej Uniwersytetu Jagiellońskiego. Przełączniki umieszczone w Centralnym Punkcie Dystrybucyjnym oraz przełączniki 10 Gigabit Ethernet znajdujące się w niektórych piętrowych punktach dystrybucyjnych muszą wspierać mechanizmy pozwalające traktowanie wszystkich tych przełączników jako jednego „systemu” (Fabric) oferującego serwisy L2, L3 i wspierające uruchomienie serwisów multicast bez konieczności konfiguracji routingu multicast np. PIM-SM, PIM-SSM. Przełączniki powyższe muszą zapewniać możliwość budowy dowolnej topologii połączeń w ramach „systemu” (Fabric), zapewniającej redundancję oraz wykorzystanie wszystkich połączeń w ramach tak zbudowanej infrastruktury. Przyłączanie konkretnych sieci wirtualnych znajdujących się na przełącznikach Gigabit Ethernet w piętrowych punktach dystrybucyjnych, do serwisów L2, L3 i serwisów multicast musi się odbywać bez konieczności konfiguracji „systemu” (Fabric) – konfiguracja musi odbywać się na przełącznikach Gigabit Ethernet znajdujących się w piętrowych punktach dystrybucyjnych w przypadku konfiguracji statycznych lub w systemie kontroli dostępu w przypadku dynamicznego przydzielania sieci VLAN.

Wszystkie przełączniki w punktach dystrybucyjnych muszą być skonfigurowane w ten sam sposób tzn. muszą mieć uruchomione uwierzytelnianie do sieci z wykorzystaniem protokołu IEEE 802.1x oraz adresów MAC. Konfiguracja taka ma zapewnić brak konieczności indywidualnego konfigurowania poszczególnych portów w przełącznikach znajdujących się w piętrowych punktach dystrybucyjnych i przeniesienie całej kontroli portów przełączników piętrowych do centralnego systemu kontroli dostępu. System kontroli dostępu będzie korzystał z uwierzytelniania bazującego na bazie danych użytkowników dostępnej w Dziale Infrastruktury Systemów Informatycznychza pomocą protokołów OpenId Connect lub SAML 2. System kontroli dostępu musi udostępniać możliwość tworzenia lokalnych grup użytkowników i urządzeń oraz nadawanie im unikalnych Polityk Bezpieczeństwa. Infrastruktura sieciowa musi zapewniać mechanizmy pozwalające automatycznie kreować serwisy L2 bez konieczności ręcznej konfiguracji przełączników piętrowych czy też przełączników szkieletowych oraz pozwalać na automatyczne przydzielanie klientów do serwisów L3 oraz serwisów typu Multicast. Przełączniki Gigabit Ethernet znajdujące się w piętrowych punktach dystrybucyjnych muszą zapewniać możliwość automatycznego wytworzenia sieci VLAN w przypadku jej braku na przełączniku i automatycznego dołączenia tej sieci do serwisów oferowanych przez „system” (Fabric).

Nowa infrastruktura sieciowa LAN musi być uzupełniona o sieć bezprzewodową pracującą w najnowszym standardzie WiFi6. Ze względu na dostępność klientów bezprzewodowych oraz realne potrzeby planowany jest zakup dwuradiowych punktów dostępowych 2x2:2 MIMO. Punkty dostępowe będą dołączone do nowo budowanej infrastruktury sieciowej i musza pracować w trybie „local bridge”, gdzie cały ruch od klientów po ich uwierzytelnieniu i autoryzacji, będzie transmitowany z sieci bezprzewodowej bezpośrednio do odpowiednich sieci VLAN skonfigurowanych na przełącznikach znajdujących się w piętrowych punktach dystrybucyjnych. Zarządzenie siecią bezprzewodową musi odbywać się centralnie z dwóch odpornych na awarie kontrolerów sieci bezprzewodowej. Kontrolery sieci bezprzewodowej będą umieszczone w Centralnym Punkcie Dystrybucyjnym i dołączone do dwóch różnych przełączników sieciowych za pomocą łączy 10 Gigabit Ethernet. Kontrolery bezprzewodowe mogą być dostarczone w postaci sprzętowej – dedykowanych urządzeń sieciowych instalowanych w szafie Rack 19” lub w postaci maszyn wirtualnych pracujących w środowisku wirtualizacyjnym. Zamawiający posiada środowisko wirtualne o parametrach określonych w pkt. 4 pt. Opis systemu wirtualizacyjnego, które może być wykorzystane na potrzeby instalacji kontrolerów bezprzewodowych jak również innych komponentów oprogramowania wymaganych w SWZ. Jeśli posiadane środowisko wirtualne nie spełnia wymagań to Oferent zobowiązany jest do dostarczenia odpowiednich dedykowanych urządzeń sprzętowych. Punkty dostępowe będą dołączane do infrastruktury sieci LAN, która realizuje uwierzytelnianie dołączanych urządzeń z wykorzystaniem IEEE 802.1x i/lub uwierzytelnianiem MAC we współpracy z systemem kontroli dostępu. Punkty dostępowe muszą zapewniać wszelkie mechanizmy pozwalające na ich uwierzytelnienie na przełączniku piętrowym z wykorzystaniem IEEE 802.1x i protokołów EAP: PEAP oraz EAP-TLS. Infrastruktura sieciowa musi zapewnić prawidłowe uwierzytelnianie punktów dostępowych z w/w protokołami oraz przydzielenie odpowiedniej Polityki Bezpieczeństwa.

Polityki Bezpieczeństwa na przełącznikach musi zapewnić m.in. przydział sieci VLAN, do których będą dostawać się klienci sieci bezprzewodowej, automatyczną sygnalizację sieci bez konieczności indywidualnej konfiguracji portu przełącznika – zmiana urządzenia dołączonego do przełącznika musi być automatycznie wykrywana przez infrastrukturę sieciową i z wykorzystaniem systemu kontroli dostępu musi następować automatyczna konfiguracja portu na przełączniku piętrowym.

Rozmieszczenie punktów dostępowych sieci bezprzewodowej musi być poprzedzone pomiarami propagacji w obiekcie i stworzeniem modelu predykcyjnego sieci bezprzewodowej w jednym z dwóch systemów do projektowania sieci bezprzewodowych, zamawiający sugeruję wykorzystanie narzędzi firmy Ekahau lub Air Magnet, ze względu na znajomość tego środowiska i możliwość eksportowania wyników do innego oprogramowania, z którego zamawiający korzysta do innych celów projektowych. Dokumentacja projektu sieci bezprzewodowej staje się własnością Zamawiającego i musi być dołączona do kompletu dokumentacji powykonawczej. Szczegóły wymagań pokrycia obiektu siecią bezprzewodową zostaną opisane w pkt. 5 pt. Wymagania sieci bezprzewodowej do niniejszego SiWZ.

Nowo projektowana infrastruktura sieci przewodowej LAN i bezprzewodowej WLAN musi być uzupełniona o System Zarządzający, System Kontroli Dostępu oraz System Analizy Aplikacji działających w sieci LAN oraz WLAN. Każde powyższe oprogramowanie zarządzające może być dostarczone w postaci dedykowanego urządzenia sprzętowego z zainstalowanym oprogramowaniem lub jako maszyna wirtualna i uruchomiona na środowisku wirtualnym dostarczonym przez Zamawiającego o parametrach określonych w pkt. 4 pt. Opis systemu wirtualizacyjnego. System Kontroli Dostępu jako element krytyczny musi być wyposażony w pełną odporność na awarie – uszkodzenie pojedynczego elementu sprzętowego lub programowego nie może wpływać na ograniczenie dostępu użytkowników do sieci LAN oraz WLAN.

Cała infrastruktura sieci LAN oraz WLAN będzie dołączona do reszty infrastruktury sieci oraz serwisów udostępnianych przez Dział Infrastruktury Systemów Informatycznych. Niektóre serwisy dostępne w sieci LAN i WLAN będą połączone bezpośrednio z infrastrukturą UJ, a część z nich będzie dołączona poprzez odporny na awarie klaster Firewall. Klaster Firewall musi być dołączony do dwóch przełączników szkieletowych znajdujących się w Centralnym Punkcie Dystrybucyjnym za pomocą interfejsów sieciowych min. 40 Gigabit Ethernet.

Wszystkie urządzenia sieci LAN (łącznie z optyką) oraz WLAN wraz z Oprogramowaniem Zarządzającym, Systemem Kontroli Dostępu oraz Systemem Analizy Aplikacji muszą pochodzić od jednego producenta.

Wszystkie urządzenia muszą pochodzić z legalnego kanału sprzedaży na terenie Polski co musi być potwierdzone przez przedstawicielstwo producenta na terenie Polski.

Wszystkie urządzenia muszą być objęte 3 letnią gwarancją wymiany sprzętu w przypadku awarii na następny dzień roboczy.

1. **Szczegółowy opis przedmiotu zamówienia**
	1. **Przełączniki Gigabit Ethernet**

Poniższa tabela przedstawia wymagania dotyczące liczby portów Gigabit Ethernet 10/100/1000Base-T w poszczególnych piętrowych punktach dystrybucyjnych.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa punktu dystrybucyjnego** | **Liczba portów 10/100/1000Base-T** |
| **1.** | IDF A  | 384 portów  |
| **2.** | IDF B  | 384 porty  |
| **3.** | IDF C  | 384 porty  |
| **4.** | IDF D  | 144 porty  |
| **5.** | IDF E  | 96 portów  |
| **6.** | IDF NMR  | 24 portów  |
| **7.** | IDF Bioinformatycy  | 48 portów  |
| **8.** | IDF Horizon  | 48 portów  |
| **9.** | IDF Sekretariat  | 48 portów  |
| **10.** | IDF Trójkąt  | 24 porty  |
| **11.** | IDF Szatnia  | * 1. orty
 |

**2.1.1 Wymagania szczegółowe na przełączniki Gigabit Ethernet 10/100/1000Base-T do piętrowych punktów dystrybucyjnych**

1. Przełącznik przeznaczony do montażu w szafie Rack 19” o wysokości 1RU.
2. Przełącznik wyposażony w zasilacz 230V oraz możliwość instalacji drugiego zasilacza zapewniającego odporność na awarie.
3. Przełącznik wyposażony w 24 lub 48 portów Gigabit Ethernet 10/100/1000Base-T z zasilaniem przez skrętkę PoE+ zgodnym ze standardem IEEE 802.3at (30W).
4. Przełącznik wyposażony w 4 porty uplink SFP+.
5. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet.
6. 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.
7. Budżet mocy PoE+ z pojedynczym zasilaczem min. 380W dla wersji 24 portowej oraz 740W dla wersji 48 portowej.
8. Przełącznik musi posiadać dedykowany port Out of Band do zarządzania poza pasmem
9. Przełącznik musi posiadać dedykowany port konsoli szeregowej RS-232 lub USB
10. Przełącznik musi posiadać port USB pozwalający na podłączenie przenośnej pamięci Flash i przenoszenie plików konfiguracyjnych oraz aktualizację oprogramowania przełącznika.
11. Przełącznik musi posiadać możliwość łączenia przełączników w stos z wykorzystaniem dedykowanych portów stakujących. Porty stakujące musza posiadać przepustowość min. 10 Gb/s i zapewniać połączenie wszystkich urządzeń w stosie w sposób odporny na awarie np. w architekturze pierścienia.
12. Przełącznik musi zapewniać możliwość budowania stosu do 8 urządzeń. Stos urządzeń musi być zarządzany z pojedynczego adresu IP, musi zapewniać możliwość realizacji połączeń Link Aggregation IEEE 802.3ad z różnych przełączników w stosie.
13. Przełącznik musi zapewniać temperaturę pracy w zakresie od 0o do 50o C.
14. Przełącznik musi być wyposażony w pamięć operacyjną min. 1 GB RAM.
15. Przełącznik musi być wyposażony w pamięć Flash min. 1 GB Flash.
16. Przełącznik musi zapewniać nieblokującą architekturę o wydajności min. 200 Gb/s dla przełącznika w wersji 24 portowej oraz min. 250Gb/s dla przełącznika w wersji 48 portowej
17. Przełącznik musi zapewniać szybkość przełączania na poziomie min. 150 milionów pakietów na sekundę dla wersji 24 portowej oraz min. 190 milionów pakietów na sekundę dla wersji 48 portowej.
18. Przełącznik musi posiadać tablicę MAC adresów na min. 30 tys. wpisów
19. Przełącznik musi obsługiwać pełen zakres 4094 sieci wirtualnych zgodny z IEEE 802.1Q.
20. Przełącznik musi zapewniać obsługę Q-in-Q IEEE 802.1ad.
21. Przełącznik musi zapewniać obsługę protokołów STP:
22. STP (Spanning Tree Protocol) IEEE 802.1D
23. RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
24. PVST+ (Per-VLAN Spanning Tree Protocol)
25. MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
26. Przełącznik musi zapewniać możliwość obsługi agregacji wielu połączeń fizycznych w jedno połączenie logiczne IEEE 802.3ad wraz z obsługą LACP
27. Przełącznik musi zapewniać obsługę MCLAG (Multi Chassis Link Aggregation) pozwalającą na realizację standardowego połączenia Link Aggregation IEEE 802.3ad do pary niezależnych przełączników nie będących w stosie.
28. Przełącznik musi zapewniać obsługę MCLAG z możliwością uruchomienia protokołu LACP.
29. Przełącznik musi zapewniać obsługę QoS (Quality of Service).
30. Rozpoznawanie i realizacja priorytetów w ramach IEEE 802.1p.
31. Rozpoznawanie i realizacja priorytetów w ramach DiffServ.
32. Możliwość zmiany priorytetu dla ruchu wybranego w ramach ACL (Access Control List).
33. Możliwość ustawienia priorytetu dla portu.
34. Możliwość ustawienia priorytetu dla sieci VLAN.
35. Obsługa min. 8 kolejek priorytetów na każdym porcie przełącznika.
36. Obsługa kolejek Strict Priority.
37. Obsługa kolejek Weighted Round Robin.
38. Przełącznik musi zapewniać obsługa LLDP (Link Layer Discovery Protocol) IEEE 802.1AB.
39. Przełącznik musi zapewniać obsługę LLDP-MED (LLDP Media Endpoint Discovery).
40. Przełącznik musi zapewniać obsługę CDP
41. Przełącznik musi być wyposażony w modularny system operacyjny zapewniający podział zadań na procesy z ochroną pamięci i procesów.
42. Przełącznik musi zapewniać możliwość kontroli procesów na przełączniku – start, stop, restart
43. Przełącznik musi zapewniać możliwość instalacji min. 2 wersji oprogramowania.
44. Przełącznik musi zapewniać możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash. Przełącznik musi pozwalać na uruchomienie przełącznika ze wskazanego pliku konfiguracyjnego.
45. Przełącznik musi zapewniać możliwość monitorowania i raportowania zajętości CPU.
46. Przełącznik musi zapewniać możliwość monitorowania i raportowania zajętości pamięci.
47. Przełącznik musi zapewniać lokalną i zdalną możliwość monitoringu pakietów – Local and Remote Mirroring. Wybór monitorowanego ruchu musi być możliwy z wykorzystaniem ACL.
48. Przełącznik musi zapewniać sprzętową realizację routingu IPv4
49. Przełącznik musi zapewniać pojemność tabeli routingu IPv4 min. 12 tys wpisów
50. Przełącznik musi zapewniać sprzętową obsługę routingu IPv6
51. Przełącznik musi zapewniać pojemność tabeli routingu IPv6 min. 6 tys. wpisów
52. Przełącznik musi zapewniać obsługę routingu statycznego IPv4 oraz IPv6
53. Przełącznik musi zapewniać obsługę routingu dynamicznego RIPv1/v2 oraz RIPng
54. Przełącznik musi zapewniać obsługę routingu OSPFv2 oraz OSPFv3
55. Przełącznik musi zapewniać obsługę routingu BGPv4 – możliwość rozszerzenia przez licencje lub wymianę oprogramowania
56. Przełącznik musi zapewniać obsługa routingu IS-IS – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
57. Przełącznik musi realizować redundancję bramy z wykorzystaniem protokołu VRRP (Virtual Router Redundancy Protocol)
58. Przełącznik musi zapewniać realizację sterowania routingiem - Policy Based Routing dla IPv4 oraz IPv6
59. Przełącznik musi zapewniać obsługę statycznego przyłączania do grupy multicast
60. Przełącznik musi zapewniać filtrowanie IGMP
61. Przełącznik musi zapewniać obsługę routingu multicast PIM-SM – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
62. Przełącznik musi zapewniać obsługę Obsługa routingu multicast PIM-SSM – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
63. Przełącznik musi zapewniać obsługę IGMP v1 – RFC 1112
64. Przełącznik musi zapewniać obsługę IGMP v2 – RFC 2236
65. Przełącznik musi zapewniać obsługę IGMP v3 – RFC 3376
66. Przełącznik musi zapewniać obsługę IGMP v1/v2/v3 snooping
67. Przełącznik musi zapewniać obsługę MLDv1 (Multicast Listener Discovery version 1)
68. Przełącznik musi zapewniać obsługę MLDv2 (Multicast Listener Discovery version 2)
69. Przełącznik musi zapewniać obsługę logowania do sieci
70. Uwierzytelnianie i autoryzacja IEEE 802.1x
71. Uwierzytelnianie i autoryzacja MAC
72. Uwierzytelnianie i autoryzacja poprzez Captive Portal
73. Captive Portal uruchomiony na przdełączniku
74. Przekierowanie ruchu na zewnętrzny Captive Portal uruchomiony na systemie kontroli dostępu
75. Przełącznik musi zapewniać obsługę uwierzytelniania wielu klientów na pojedynczym porcie fizycznym (Multiple Supplicant)
76. Przełącznik musi zapewniać obsługę uwierzytelniania i autoryzacji IEEE 802.1x oraz MAC na portach pracujących w trybie Link Aggregation
77. Przełącznik musi zapewniać obsługę autoryzacji z przydziałem dla każdego uwierzytelnionego klienta:
78. sieci VLAN – pojedynczy VLAN „nietagowany”, wiele VLAN „tagowanych” IEEE 802.1Q – przykładowo uwierzytelnienie i autoryzacja punktu dostępowego zarządzanego w sieci VLAN „nietagowanej”, który będzie obsługiwał klientów bezprzewodowych dołączanych do różnych sieci VLAN „tagowanych”, które muszą być dostępne na porcie przełącznika po uwierzytelnieniu i autoryzacji punktu dostępowego
79. ACL – listy kontroli dostępu pozwalające na filtrację ruchu od uwierzytelnionego klienta do sieci
80. Quality of Service – przydział priorytetów dla całego ruchu uwierzytelnionego urządzenia (np. telefon VoIP dołączony do portu) oraz przydział priorytetów dla ruchu wybranego za pomocą ACL (np. konkretny protokół TCP, UDP lub zakres portów TCP, UDP)
81. IEEE 802.1Qcj – sieć VLAN wraz z identyfikatorem serwisu w Fabric
82. Przełącznik musi zapewniać obsługę selektywnej obsługi wymuszenia ponownej autoryzacji w celu jej zmiany (sieć VLAN, ACL, Quality of Service) bez konieczności wyłączania i włączania portu – CoA RFC 5176
83. Przełącznik musi zapewniać obsługę automatyzacji przyłączania urządzeń sieciowych obsługujących protokół LLDP – przykładowo możliwość sprawdzenia informacji o dołączanym do portu urządzeniu poprzez odczytanie otrzymywanych informacji LLDP i na jej podstawie odpowiednia konfiguracja portu przełącznika - VLAN, ACL, Quality of Service
84. Przełącznik musi zapewniać obsługę dwukierunkowych (ingress oraz egress) list kontroli dostępu ACL pracujących na warstwie 2, 3 i 4. Listy ACL muszą zapewniać możliwość klasyfikacji ruchu na podstawie następujących parametrów:
85. Adres MAC źródłowy i docelowy z maską
86. Adres IP źródłowy i docelowy z maską
87. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF itp.
88. Numery portów źródłowych i docelowych TCP, UDP
89. Zakresy portów źródłowych i docelowych TCP, UDP
90. Identyfikator sieci VLAN – VLAN ID IEEE 802.1Q
91. Quality of Service – priorytet IEEE 802.1p oraz DiffServ
92. Flagi TCP
93. Obsługa fragmentów
94. Wszystkie powyższe listy kontroli dostępu muszą być realizowane w sprzęcie i nie mogą wpływać na wydajność przełączanego ruchu sieciowego
95. Przełącznik musi zapewniać obsługę ograniczania przepustowości (rate limit) dla ruchu wybranego listą kontroli dostępu ACL
96. Przełącznik musi zapewniać obsługę ograniczania przepustowości (rate limit) na fizyczny porcie przełącznika
97. Przełącznik musi zapewniać obsługę możliwości zliczania pakietów trafiających do listy kontroli dostępu ACL
98. Przełącznik musi zapewniać obsługę możliwość wykorzystania informacji o zliczanych pakietów trafiających do listy kontroli dostępu ACL do automatycznej reakcji przełącznika:
99. Zablokowania ruchu – np. przekroczenie ustalonej liczby pakietów ICMP w ciągu 5 sekund (wykrywanie i obrona sieci przed atakiem Ping of Death), przekroczenie ustalonej liczby pakietów TCP Syn (wykrywanie i obrona przed atakiem Syn Flood)
100. Przekierowanie ruchu do kolejki o niższym priorytecie
101. Wysłanie trapu SNMP do platformy zarządzającej – np. zawierającego informację o ataku Ping of Death lub Syn Flood
102. Wysyłanie zdarzenia do systemu logowania SYSLOG z możliwością własnego opisu zdarzenia
103. Możliwość wykonania dowolnej komendy CLI lub uruchomienia skryptu CLI
104. Przełącznik musi zapewniać obsługę konfiguracji min. 8 tys. reguł ACL na wejściu i 1 tys. reguł ACL na wyjściu
105. Przełącznik musi zapewniać zabezpieczenie systemu operacyjnego przed atakami DoS
106. Automatyczna filtracja źródła DoS – Network Ingress Filtering RFC 2267
107. Zabezpieczenie przed atakami SYN – SYN Attack Protection
108. Przełącznik musi zapewniać obsługę mechanizmów bezpieczeństwa związanych z DHCP Serwerem
109. Zabezpieczenie przed przydzielaniem adresów IP przez nieautoryzowany serwer DHCP – Trusted DHCP Server
110. Monitorowanie przydziału adresów IP przez DHCP serwer – DHCP Snooping
111. Zabezpieczenie przed konfiguracją statycznego adresu IP. Tylko komputer z adresem IP przydzielonym przez autoryzowany serwer DHCP może dostać się do sieci – IP Source Guard
112. Przełącznik musi zapewniać obsługę zabezpieczeń protokołu ARP – ARP Inspection, ARP Validation, DHCP Secured ARP
113. Przełącznik musi zapewniać obsługę mechanizmów wykrywania aplikacji na warstwie 7 przy współpracy z zewnętrznym systemem Analizy Aplikacji
114. Przełącznik musi zapewniać obsługę wysyłania zdarzeń systemowych z przełącznika do zewnętrznego systemu logowania SYSLOG.
115. Przełącznik musi zapewniać obsługę konfiguracji wielu systemów SYSLOG pozwalających na selektywne wysyłanie zdarzeń do różnych systemów logujących – np. zdarzenia związane z bezpieczeństwem powinny trafić do systemu SIEM lub działu bezpieczeństwa, a zdarzenia związane z np. uszkodzeniem wentylatora, łącza fizycznego, przekroczoną temperaturą lub restartem procesu powinny trafić do lokalnego administratora.
116. Przełącznik musi zapewniać obsługę skryptów CLI na przełączniku
117. Przełącznik musi zapewniać obsługę skryptów Python na przełączniku
118. Możliwość uruchomienia skryptu Python jako własnego procesu działającego również po restarcie przełącznika
119. Przełącznik musi zapewniać obsługę uruchamiania skryptów CLI oraz Python:
120. Ręcznie – przez administratora
121. O określonym czasie – automatycznie o zdefiniowanym dniu i godzinie
122. Co wskazany czas – automatycznie np. codziennie o godzinie 8
123. Na podstawie wpisów w logu systemowym – automatycznie po pojawieniu się konkretnego zdarzenia w logu systemowym
124. Edycja skryptów musi być możliwa bezpośrednio na przełączniku za pomocą wbudowanego edytora
125. Przełącznik musi zapewniać obsługę wykrywania periodycznego zaniku linku (Port Flap) z możliwością definicji liczby zdarzeń w określonym czasie i po przekroczeniu ustalonego poziomu podjęcie akcji polegającej na:
126. Permanentnym wyłączeniu portu
127. Czasowym wyłączeniu portu z możliwością definicji czasu
128. Wysłaniem zdarzenia do logu systemowego i SYSLOG
129. Wysłaniem trapu SNMP do platformy zarządzającej
130. Przełącznik musi być wyposażony w protokoły administracyjne:
131. SSHv2 klient i serwer – IPv4 oraz IPv6
132. Ping – IPv4 oraz IPv6
133. Traceroute – IPv4 oraz IPv6
134. Synchronizacja czasu systemowego SNTP lub NTP wraz z obsługą strefy czasowej i możliwości definicji automatycznej zmiany czasu z letniego na zimowy i odwrotnie.
135. Zarządzanie przez przeglądarkę www za pomocą protokołu https
136. Obsługa uwierzytelniania za pomocą certyfikatów X509v3 dla bezpiecznego logowania SSH
137. Transfer plików za pomocą:
138. SFTP i/lub SCP
139. TFTP
140. Obsługa protokołu RADIUS Authentication (RFC 2138)
141. Obsługa protokołu RADIUS Accounting (RFC 2139)
142. Obsługa per-command RADIUS Authentication
143. Obsługa TACACS+
144. Możliwość uruchomienia DHCP serwera na wskazanych sieciach VLAN
145. Możliwość uruchomienia klienta DHCP na wskazanych sieciach VLAN
146. Przełącznik musi wspierać mechanizmy automatycznego dołączenia sieci VLAN do „systemu” Fabric z wykorzystaniem standardowego rozwiązania IEEE 802.Qcj (Automatic Attachment to Provider Backbone)
147. Rozwiązanie musi zapewniać wsparcie IEEE 802.Qcj dla statycznej oraz dynamicznej konfiguracji sieci VLAN:
148. Konfiguracja statyczna ma polegać na mapowaniu sieci VLAN do identyfikatora serwisu w Fabric
149. konfiguracja dynamiczna ma polegać na odebraniu informacji o sieci VLAN oraz identyfikatorze serwisu z systemu kontroli dostępu (podczas logowania IEEE 802.1x lub uwierzytelniania MAC) i na tej podstawie wytworzeniu sieci VLAN, jeśli nie istnieje na przełączniku brzegowym, przydzielenia tej sieci do autoryzowanego portu i do wszystkich portów dołączonych do Fabric

1. **Przełączniki 10 Gigabit Ethernet.**

Poniższa tabela przedstawia wymagania dotyczące liczby portów 10 Gigabit Ethernet w poszczególnych piętrowych punktach dystrybucyjnych z podziałem na porty na skrętkę 1/2.5/5/10GBase-T oraz porty 1/10G SFP+.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa punktu dystrybucyjnego** | **Liczba portów 1/2.5/5/10GBase-T** | **Liczba portów 1/10G SFP+** |
| **1.** | IDF A  | 12  | 12  |
| **2.** | IDF B  | 12  | 12  |
| **3.** | IDF C  | 12  | 12  |
| **4.** | IDF D  | -  | -  |
| **5.** | IDF E  | 12  | 12  |
| **6.** | IDF NMR  | 12  | 12  |
| **7.** | IDF Bioinformatycy  | 12  | 12  |
| **8.** | IDF Horizon  | 12  | 12  |
| **9.** | IDF Sekretariat  | -  | -  |
| **10.** | IDF Trójkąt  | -  | -  |
| **11.** | IDF Szatnia  | -  | -  |

1. **Wymagania szczegółowe na przełączniki 10 Gigabit Ethernet w piętrowych punktach dystrybucyjnych**

1. Przełącznik przeznaczony do montażu w szafie Rack 19” o wysokości 1RU.
2. Przełącznik wyposażony w zasilacz 230V oraz możliwość instalacji drugiego zasilacza zapewniającego odporność na awarie.
3. Przełącznik wyposażony w 12 portów 10 Gigabit Ethernet 1/2.5/5/10GBase-T z zasilaniem przez skrętkę PoE+ zgodnym ze standardem IEEE 802.3bt (60W) oraz 12 portów 10 Gigabit Ethernet 1/10G SFP+
4. Przełącznik wyposażony w dodatkowe 4 porty SFP28 z obsługą wkładek o przepustowości 25 Gb/s lub QSFP+/QSFP28 z obsługą portów 40 lub 100G (wybór zależy od zaproponowanego przełącznika w Centralnym Punkcie Dystrybucyjnym)
5. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet.
6. 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.
7. Budżet mocy PoE+ min 720 W.
8. Przełącznik musi posiadać dedykowany port Out of Band do zarządzania poza pasmem
9. Przełącznik musi posiadać dedykowany port konsoli szeregowej RS-232 lub USB
10. Przełącznik musi posiadać port USB pozwalający na podłączenie przenośnej pamięci Flash i przenoszenie plików konfiguracyjnych oraz aktualizację oprogramowania przełącznika.
11. Przełącznik musi zapewniać temperaturę pracy w zakresie od 0o do 45o C.
12. Przełącznik musi być wyposażony w pamięć operacyjną min. 8 GB RAM.
13. Przełącznik musi być wyposażony w pamięć Flash min. 8 GB Flash.
14. Przełącznik musi zapewniać nieblokującą architekturę o wydajności min. 680 Gb/s.
15. Przełącznik musi zapewniać szybkość przełączania na poziomie min. 500 milionów pakietów na sekundę.
16. Przełącznik musi posiadać tablicę MAC adresów na min. 80 tys. wpisów
17. Przełącznik musi obsługiwać pełen zakres 4 tys. sieci wirtualnych zgodny z IEEE 802.1Q.
18. Przełącznik musi zapewniać obsługę protokołów STP:
19. RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
20. MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
21. Przełącznik musi zapewniać możliwość obsługi agregacji wielu połączeń fizycznych w jedno połączenie logiczne IEEE 802.3ad wraz z obsługą LACP
22. Przełącznik musi zapewniać obsługę MCLAG (Multi Chassis Link Aggregation) pozwalającą na realizację standardowego połączenia Link Aggregation IEEE 802.3ad do pary niezależnych przełączników nie będących w stosie.
23. Przełącznik musi zapewniać obsługę MCLAG z możliwością uruchomienia protokołu LACP.
24. Przełącznik musi zapewniać obsługę QoS (Quality of Service).
25. Rozpoznawanie i realizacja priorytetów w ramach IEEE 802.1p.
26. Rozpoznawanie i realizacja priorytetów w ramach DiffServ.
27. Możliwość zmiany priorytetu dla ruchu wybranego w ramach ACL (Access Control List).
28. Możliwość ustawienia priorytetu dla portu.
29. Możliwość ustawienia priorytetu dla sieci VLAN.
30. Obsługa min. 8 kolejek priorytetów na każdym porcie przełącznika.
31. Obsługa kolejek Strict Priority.
32. Obsługa kolejek Weighted Round Robin.
33. Przełącznik musi zapewniać obsługa LLDP (Link Layer Discovery Protocol) IEEE 802.1AB.
34. Przełącznik musi zapewniać obsługę LLDP-MED (LLDP Media Endpoint Discovery).
35. Przełącznik musi zapewniać obsługę CDP
36. Przełącznik musi zapewniać możliwość instalacji min. 2 wersji oprogramowania.
37. Przełącznik musi zapewniać możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash. Przełącznik musi pozwalać na uruchomienie przełącznika ze wskazanego pliku konfiguracyjnego.
38. Przełącznik musi zapewniać możliwość monitorowania i raportowania zajętości CPU.
39. Przełącznik musi zapewniać możliwość monitorowania i raportowania zajętości pamięci.
40. Przełącznik musi zapewniać lokalną i zdalną możliwość monitoringu pakietów – Local and Remote Mirroring. Wybór monitorowanego ruchu musi być możliwy z wykorzystaniem ACL.
41. Przełącznik musi zapewniać sprzętową realizację routingu IPv4
42. Przełącznik musi zapewniać pojemność tabeli routingu IPv4 min. 12 tys wpisów
43. Przełącznik musi zapewniać sprzętową obsługę routingu IPv6
44. Przełącznik musi zapewniać pojemność tabeli routingu IPv6 min. 6 tys. wpisów
45. Przełącznik musi zapewniać obsługę routingu statycznego IPv4 oraz IPv6
46. Przełącznik musi zapewniać obsługę routingu dynamicznego RIPv1/v2 oraz RIPng
47. Przełącznik musi zapewniać obsługę routingu OSPFv2 oraz OSPFv3
48. Przełącznik musi zapewniać obsługę routingu BGPv4
49. Przełącznik musi zapewniać obsługa routingu IS-IS
50. Przełącznik musi realizować redundancję bramy z wykorzystaniem protokołu VRRP (Virtual Router Redundancy Protocol)
51. Przełącznik musi zapewniać obsługę statycznego przyłączania do grupy multicast
52. Przełącznik musi zapewniać filtrowanie IGMP
53. Przełącznik musi zapewniać obsługę routingu multicast PIM-SM – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
54. Przełącznik musi zapewniać obsługę Obsługa routingu multicast PIM-SSM – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
55. Przełącznik musi zapewniać obsługę IGMP v1 – RFC 1112
56. Przełącznik musi zapewniać obsługę IGMP v2 – RFC 2236
57. Przełącznik musi zapewniać obsługę IGMP v3 – RFC 3376
58. Przełącznik musi zapewniać obsługę IGMP v1/v2/v3 snooping
59. Przełącznik musi zapewniać obsługę MLDv1 (Multicast Listener Discovery version 1)
60. Przełącznik musi zapewniać obsługę MLDv2 (Multicast Listener Discovery version 2)
61. Przełącznik musi zapewniać obsługę logowania do sieci
62. Uwierzytelnianie i autoryzacja IEEE 802.1x
63. Uwierzytelnianie i autoryzacja MAC
64. Przełącznik musi zapewniać obsługę uwierzytelniania wielu klientów na pojedynczym porcie fizycznym (Multiple Supplicant)
65. Przełącznik musi zapewniać obsługę autoryzacji z przydziałem dla każdego uwierzytelnionego klienta:
66. sieci VLAN
67. ACL
68. Przełącznik musi zapewniać obsługę selektywnej obsługi wymuszenia ponownej autoryzacji w celu jej zmiany (sieć VLAN, ACL) bez konieczności wyłączania i włączania portu – CoA RFC 5176
69. Przełącznik musi zapewniać obsługę dwukierunkowych (ingress oraz egress) list kontroli dostępu ACL pracujących na warstwie 2, 3 i 4. Listy ACL muszą zapewniać możliwość klasyfikacji ruchu na podstawie następujących parametrów:
70. Adres MAC źródłowy i docelowy z maską
71. Adres IP źródłowy i docelowy z maską
72. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF itp.
73. Numery portów źródłowych i docelowych TCP, UDP
74. Zakresy portów źródłowych i docelowych TCP, UDP lub maska dla portów
75. Identyfikator sieci VLAN – VLAN ID IEEE 802.1Q
76. Quality of Service – priorytet IEEE 802.1p oraz DiffServ
77. Flagi TCP
78. Obsługa fragmentów
79. Wszystkie powyższe listy kontroli dostępu muszą być realizowane w sprzęcie i nie mogą wpływać na wydajność przełączanego ruchu sieciowego
80. Przełącznik musi zapewniać obsługę ograniczania przepustowości (rate limit) na fizyczny porcie przełącznika
81. Przełącznik musi zapewniać obsługę możliwości zliczania pakietów trafiających do listy kontroli dostępu ACL
82. Przełącznik musi zapewniać obsługę konfiguracji min. 1 tys. reguł ACL na wejściu i 240 reguł ACL na wyjściu
83. Przełącznik musi zapewniać zabezpieczenie systemu operacyjnego przed atakami DoS
84. Przełącznik musi zapewniać obsługę mechanizmów bezpieczeństwa związanych z DHCP Serwerem
85. Zabezpieczenie przed przydzielaniem adresów IP przez nieautoryzowany serwer DHCP – Trusted DHCP Server
86. Monitorowanie przydziału adresów IP przez DHCP serwer – DHCP Snooping
87. Zabezpieczenie przed konfiguracją statycznego adresu IP. Tylko komputer z adresem IP przydzielonym przez autoryzowany serwer DHCP może dostać się do sieci – IP Source Guard
88. Przełącznik musi zapewniać obsługę zabezpieczeń protokołu ARP – ARP Inspection, ARP Validation, DHCP Secured ARP
89. Przełącznik musi zapewniać obsługę mechanizmów wykrywania aplikacji na warstwie 7 przy współpracy z zewnętrznym systemem Analizy Aplikacji
90. Przełącznik musi zapewniać obsługę wysyłania zdarzeń systemowych z przełącznika do zewnętrznego systemu logowania SYSLOG.
91. Przełącznik musi zapewniać obsługę konfiguracji wielu systemów SYSLOG pozwalających na selektywne wysyłanie zdarzeń do różnych systemów logujących
92. Przełącznik musi zapewniać obsługę wykrywania periodycznego zaniku linku (Port Flap) z możliwością definicji liczby zdarzeń w określonym czasie i po przekroczeniu ustalonego poziomu podjęcie akcji polegającej na:
93. Permanentnym wyłączeniu portu
94. Wysłaniem zdarzenia do logu systemowego i SYSLOG
95. Wysłaniem trapu SNMP do platformy zarządzającej
96. Przełącznik musi być wyposażony w protokoły administracyjne:
97. SSHv2 klient i serwer – IPv4 oraz IPv6
98. Ping – IPv4 oraz IPv6
99. Traceroute – IPv4 oraz IPv6
100. Synchronizacja czasu systemowego SNTP lub NTP wraz z obsługą strefy czasowej i możliwości definicji automatycznej zmiany czasu z letniego na zimowy i odwrotnie.
101. Zarządzanie przez przeglądarkę www za pomocą protokołu https
102. Obsługa uwierzytelniania za pomocą certyfikatów X509v3 dla bezpiecznego logowania SSH
103. Transfer plików za pomocą:
104. SFTP i/lub SCP
105. TFTP
106. Obsługa protokołu RADIUS Authentication (RFC 2138)
107. Obsługa protokołu RADIUS Accounting (RFC 2139)
108. Obsługa TACACS+
109. Możliwość uruchomienia klienta DHCP na wskazanych sieciach VLAN
110. Przełącznik musi wspierać rozwiązanie budowania „systemu” (Fabric) z wykorzystaniem standardowego rozwiązania IEEE 802.1aq (Shortest Path Bridging)
111. Powyższy mechanizm musi zapewniać możliwość tworzenia serwisów L2, L3 oraz multicast w ramach całego „systemu” (Fabric).
112. Przełącznik musi wspierać możliwość przyłączania urządzeń, i sieci VLAN do serwisów L2, L3 i multicast, niewspierających standardu IEEE 802.1aq (Shortest Path Bridging) z wykorzystaniem standardu IEEE 802.1Qcj (Automatic Attachment to Provider Backbone)

1. **Przełączniki 10/25/40/100 Gigabit Ethernet dla Centralnego Punktu Dystrybucyjnego**

Centralny punkt dystrybucyjny musi być wyposażony w parę przełączników posiadających porty pozwalające na agregację wszystkich połączeń z piętrowych punktów dystrybucyjnych, dołączenie urządzeń dodatkowych oferowanych w ramach niniejszego postępowania takich jak system wirtualizacji lub ewentualne kontrolery sprzętowe WiFi oraz musi zapewniać połączenie z resztą infrastruktury sieci UJ z wykorzystaniem portów 10, 40 lub 100 Gigabit Ethernet.

1. **Wymagania szczegółowe na przełączniki do Centralnego Punktu Dystrybucyjnego**

1. Przełącznik przeznaczony do montażu w szafie Rack 19” o wysokości 1RU.
2. Przełącznik wyposażony w dwa zasilacz 230V zapewniające odporność na awarie w przypadku jednego z nich.
3. Przełącznik musi posiadać wymienne, odporne na awarie, zestawy wentylatorów zapewniających chłodzenie przód-tył.
4. Przełącznik musi być wyposażony w min. 48 portów 1/10/25 Gigabit Ethernet
5. Przełącznik musi być wyposażony w min. 6 portów 40/100 Gigabit Ethernet – 2 z tych portów posłużą do połączenia pary przełączników ze sobą
6. 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.
7. Przełącznik musi posiadać dedykowany port Out of Band do zarządzania poza pasmem
8. Przełącznik musi posiadać dedykowany port konsoli szeregowej RS-232 lub USB
9. Przełącznik musi posiadać port USB pozwalający na podłączenie przenośnej pamięci Flash i przenoszenie plików konfiguracyjnych oraz aktualizację oprogramowania przełącznika.
10. Przełącznik musi zapewniać temperaturę pracy w zakresie od 0o do 45o C.
11. Przełącznik musi być wyposażony w pamięć operacyjną min. 16 GB RAM.
12. Przełącznik musi być wyposażony w pamięć Flash min. 16 GB Flash.
13. Przełącznik musi zapewniać nieblokującą architekturę o wydajności min. 4 Tb/s.
14. Przełącznik musi zapewniać szybkość przełączania na poziomie min. 1 milion pakietów na sekundę.
15. Przełącznik musi posiadać tablicę MAC adresów na min. 160 tys. wpisów
16. Przełącznik musi obsługiwać pełen zakres 4 tys. sieci wirtualnych zgodny z IEEE 802.1Q.
17. Przełącznik musi zapewniać obsługę protokołów STP:
18. RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
19. MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
20. Przełącznik musi zapewniać możliwość obsługi agregacji wielu połączeń fizycznych w jedno połączenie logiczne IEEE 802.3ad wraz z obsługą LACP
21. Przełącznik musi zapewniać obsługę MCLAG (Multi Chassis Link Aggregation) pozwalającą na realizację standardowego połączenia Link Aggregation IEEE 802.3ad do pary niezależnych przełączników nie będących w stosie.
22. Przełącznik musi zapewniać obsługę MCLAG z możliwością uruchomienia protokołu LACP.
23. Przełącznik musi zapewniać obsługę QoS (Quality of Service).
24. Rozpoznawanie i realizacja priorytetów w ramach IEEE 802.1p.
25. Rozpoznawanie i realizacja priorytetów w ramach DiffServ.
26. Możliwość zmiany priorytetu dla ruchu wybranego w ramach ACL (Access Control List).
27. Możliwość ustawienia priorytetu dla portu.
28. Możliwość ustawienia priorytetu dla sieci VLAN.
29. Obsługa min. 8 kolejek priorytetów na każdym porcie przełącznika.
30. Obsługa kolejek Strict Priority.
31. Obsługa kolejek Weighted Round Robin.
32. Przełącznik musi zapewniać obsługa LLDP (Link Layer Discovery Protocol) IEEE 802.1AB.
33. Przełącznik musi zapewniać obsługę LLDP-MED (LLDP Media Endpoint Discovery).
34. Przełącznik musi zapewniać obsługę CDP
35. Przełącznik musi zapewniać możliwość instalacji min. 2 wersji oprogramowania.
36. Przełącznik musi zapewniać możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash. Przełącznik musi pozwalać na uruchomienie przełącznika ze wskazanego pliku konfiguracyjnego.
37. Przełącznik musi zapewniać możliwość monitorowania i raportowania zajętości CPU.
38. Przełącznik musi zapewniać możliwość monitorowania i raportowania zajętości pamięci.
39. Przełącznik musi zapewniać lokalną i zdalną możliwość monitoringu pakietów – Local and Remote Mirroring. Wybór monitorowanego ruchu musi być możliwy z wykorzystaniem ACL.
40. Przełącznik musi zapewniać sprzętową realizację routingu IPv4
41. Przełącznik musi zapewniać pojemność tabeli routingu IPv4 min. 12 tys wpisów
42. Przełącznik musi zapewniać sprzętową obsługę routingu IPv6
43. Przełącznik musi zapewniać pojemność tabeli routingu IPv6 min. 6 tys. wpisów
44. Przełącznik musi zapewniać obsługę routingu statycznego IPv4 oraz IPv6
45. Przełącznik musi zapewniać obsługę routingu dynamicznego RIPv1/v2 oraz RIPng
46. Przełącznik musi zapewniać obsługę routingu OSPFv2 oraz OSPFv3
47. Przełącznik musi zapewniać obsługę routingu BGPv4
48. Przełącznik musi zapewniać obsługa routingu IS-IS
49. Przełącznik musi realizować redundancję bramy z wykorzystaniem protokołu VRRP (Virtual Router Redundancy Protocol)
50. Przełącznik musi zapewniać obsługę statycznego przyłączania do grupy multicast
51. Przełącznik musi zapewniać filtrowanie IGMP
52. Przełącznik musi zapewniać obsługę routingu multicast PIM-SM – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
53. Przełącznik musi zapewniać obsługę Obsługa routingu multicast PIM-SSM – możliwość rozszerzenia przez licencję lub wymianę oprogramowania
54. Przełącznik musi zapewniać obsługę IGMP v1 – RFC 1112
55. Przełącznik musi zapewniać obsługę IGMP v2 – RFC 2236
56. Przełącznik musi zapewniać obsługę IGMP v3 – RFC 3376
57. Przełącznik musi zapewniać obsługę IGMP v1/v2/v3 snooping
58. Przełącznik musi zapewniać obsługę MLDv1 (Multicast Listener Discovery version 1)
59. Przełącznik musi zapewniać obsługę MLDv2 (Multicast Listener Discovery version 2)
60. Przełącznik musi zapewniać obsługę logowania do sieci
61. Uwierzytelnianie i autoryzacja IEEE 802.1x
62. Uwierzytelnianie i autoryzacja MAC
63. Przełącznik musi zapewniać obsługę uwierzytelniania wielu klientów na pojedynczym porcie fizycznym (Multiple Supplicant)
64. Przełącznik musi zapewniać obsługę autoryzacji z przydziałem dla każdego uwierzytelnionego klienta:
65. sieci VLAN
66. ACL
67. Przełącznik musi zapewniać obsługę selektywnej obsługi wymuszenia ponownej autoryzacji w celu jej zmiany (sieć VLAN, ACL) bez konieczności wyłączania i włączania portu – CoA RFC 5176
68. Przełącznik musi zapewniać obsługę dwukierunkowych (ingress oraz egress) list kontroli dostępu ACL pracujących na warstwie 2, 3 i 4. Listy ACL muszą zapewniać możliwość klasyfikacji ruchu na podstawie następujących parametrów:
69. Adres MAC źródłowy i docelowy z maską
70. Adres IP źródłowy i docelowy z maską
71. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF itp.
72. Numery portów źródłowych i docelowych TCP, UDP
73. Zakresy portów źródłowych i docelowych TCP, UDP lub maska dla portów
74. Identyfikator sieci VLAN – VLAN ID IEEE 802.1Q
75. Quality of Service – priorytet IEEE 802.1p oraz DiffServ
76. Flagi TCP
77. Obsługa fragmentów
78. Wszystkie powyższe listy kontroli dostępu muszą być realizowane w sprzęcie i nie mogą wpływać na wydajność przełączanego ruchu sieciowego
79. Przełącznik musi zapewniać obsługę ograniczania przepustowości (rate limit) na fizyczny porcie przełącznika
80. Przełącznik musi zapewniać obsługę możliwości zliczania pakietów trafiających do listy kontroli dostępu ACL
81. Przełącznik musi zapewniać obsługę konfiguracji min. 500 reguł ACL na wejściu i 250 reguł ACL na wyjściu
82. Przełącznik musi zapewniać zabezpieczenie systemu operacyjnego przed atakami DoS
83. Przełącznik musi zapewniać obsługę mechanizmów bezpieczeństwa związanych z DHCP Serwerem
84. Zabezpieczenie przed przydzielaniem adresów IP przez nieautoryzowany serwer DHCP – Trusted DHCP Server
85. Monitorowanie przydziału adresów IP przez DHCP serwer – DHCP Snooping
86. Zabezpieczenie przed konfiguracją statycznego adresu IP. Tylko komputer z adresem IP przydzielonym przez autoryzowany serwer DHCP może dostać się do sieci – IP Source Guard
87. Przełącznik musi zapewniać obsługę zabezpieczeń protokołu ARP – ARP Inspection, ARP Validation, DHCP Secured ARP
88. Przełącznik musi zapewniać obsługę mechanizmów wykrywania aplikacji na warstwie 7 przy współpracy z zewnętrznym systemem Analizy Aplikacji
89. Przełącznik musi zapewniać obsługę wysyłania zdarzeń systemowych z przełącznika do zewnętrznego systemu logowania SYSLOG.
90. Przełącznik musi zapewniać obsługę konfiguracji wielu systemów SYSLOG pozwalających na selektywne wysyłanie zdarzeń do różnych systemów logujących
91. Przełącznik musi zapewniać obsługę wykrywania periodycznego zaniku linku (Port Flap) z możliwością definicji liczby zdarzeń w określonym czasie i po przekroczeniu ustalonego poziomu podjęcie akcji polegającej na:
92. Permanentnym wyłączeniu portu
93. Wysłaniem zdarzenia do logu systemowego i SYSLOG
94. Wysłaniem trapu SNMP do platformy zarządzającej
95. Przełącznik musi być wyposażony w protokoły administracyjne:
96. SSHv2 klient i serwer – IPv4 oraz IPv6
97. Ping – IPv4 oraz IPv6
98. Traceroute – IPv4 oraz IPv6
99. Synchronizacja czasu systemowego SNTP lub NTP wraz z obsługą strefy czasowej i możliwości definicji automatycznej zmiany czasu z letniego na zimowy i odwrotnie.
100. Zarządzanie przez przeglądarkę www za pomocą protokołu https
101. Obsługa uwierzytelniania za pomocą certyfikatów X509v3 dla bezpiecznego logowania SSH
102. Transfer plików za pomocą:
103. SFTP i/lub SCP
104. TFTP
105. Obsługa protokołu RADIUS Authentication (RFC 2138)
106. Obsługa protokołu RADIUS Accounting (RFC 2139)
107. Obsługa TACACS+
108. Możliwość uruchomienia klienta DHCP na wskazanych sieciach VLAN
109. Przełącznik musi wspierać rozwiązanie budowania „systemu” (Fabric) z wykorzystaniem standardowego rozwiązania IEEE 802.1aq (Shortest Path Bridging)
110. Powyższy mechanizm musi zapewniać możliwość tworzenia serwisów L2, L3 oraz multicast w ramach całego „systemu” (Fabric).
111. Przełącznik musi wspierać możliwość przyłączania urządzeń, i sieci VLAN do serwisów L2, L3 i multicast, niewspierających standardu IEEE 802.1aq (Shortest Path Bridging) z wykorzystaniem standardu IEEE 802.1Qcj (Automatic Attachment to Provider Backbone)

Podział strony

1. **System bezprzewodowy WiFi6**

W ramach niniejszego postępowania wymaga się zaprojektowania i zbudowania sieci bezprzewodowej pracującej w najnowszym standardzie WiFi6 działającego z wykorzystaniem dwóch odpornych na awarie kontrolerów sieci bezprzewodowej oraz odpowiedniej liczby bezprzewodowych punktów dostępowych. Liczba punktów dostępowych będzie wynikać z projektu, który jest również częścią tego postępowania. Kontroler bezprzewodowy może być dostarczony w postaci sprzętowego urządzenia instalowanego w Centralnym Punkcie Dystrybucyjnym lub w postaci maszyny wirtualnej instalowanej na dostarczonym przez Zamawiającego systemie wirtualizacji wyposażonym w system wirtualizacji. Szczegóły dostępnego systemu wirtualizacyjnego opisane są w pkt. 4 pt. Opis systemu wirtualizacyjnego. Poniższe wymagania na kontroler są wymaganiami na system kontrolera wraz z punktami dostępowymi.

1. **Wymagania na kontroler bezprzewodowy**

1. Kontroler bezprzewodowy dostarczony jako
2. Kontroler sprzętowy w formie klastra odpornego na awarie (opcja 1)
3. Kontroler musi być przeznaczony do montażu w szafie Rack 19”
4. Kontroler musi być wyposażony w dwa zasilacz 230V zapewniające odporność na awarie w przypadku jednego z nich.
5. Kontroler musi posiadać wymienne, odporne na awarie, zestawy wentylatorów zapewniających chłodzenie przód-tył.
6. Kontroler musi być wyposażony w min. 2 porty 10 Gigabit Ethernet SFP+ do podłączenia do przełączników znajdujących się w Centralnym Punkcie Dystrybucyjnym
7. Kontroler musi być wyposażone w inne niezbędne porty, jeśli są wymagane do stworzenia odpornego na awarie klastra
8. Kontroler wirtualny (opcja 2)
9. Kontroler musi być przeznaczony do instalacji w systemie wirtualizacji.
10. Kontroler musi zapewniać alternatywnie możliwość instalacji w systemie HyperV lub OpenStack
11. Kontroler musi być zainstalowany na środowisku wirtualizacyjnym opisanym w *pkt. 4 pt.* Opis systemu wirtualizacyjnego lub niezbędne środowisko wirtualizacyjne musi być dostarczone przez Oferenta
12. Niezależnie od powyższych opcji kontroler musi być dostarczony w postaci odpornego na awarie klastra
13. Kontroler musi zapewnić skalowalność do min. 1000 punktów dostępowych
14. Kontroler musi zapewnić skalowalność niezbędną do obsługi min. 8 tys jednoczesnych użytkowników sieci bezprzewodowej.
15. Kontroler musi zapewniać obsługę sieci VLAN zgodnych z IEEE 802.1Q
16. Kontroler musi być zarządzany przez przeglądarkę www bez konieczności instalacji aplikacji na stacji zarządzającej jak np. Java
17. Kontroler musi zapewniać obsługę wielu Lokalizacji z wizualizacją ich stanu, liczby sieci bezprzewodowych (SSID) oraz liczby obsługiwanych punktów dostępowych w każdej lokalizacji.
18. 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
19. Kontroler musi zapewniać możliwość konfiguracji planów poszczególnych pięter budynków oraz umieszczenie punktów dostępowych na planie
20. Kontroler musi zapewniać możliwość nanoszenia na plany budynków ścian i pozwalać na wizualizację zasięgu poszczególnych punktów dostępowych umieszczonych na planie.
21. Kontroler musi zapewniać możliwość importu planów z systemu planowania Ekahau (ESX) jak również wczytywanie planów piętra z plików graficznych
22. Kontroler musi zapewniać widzialność wszystkich dołączonych do kontrolera punktów dostępowych z następującymi informacjami:
23. Nazwa punktu dostępowego – konfigurowalna nazwa punktu (Host Name)
24. Typ punktu dostępowego
25. Numer seryjny punktu dostępowego
26. MAC adres punktu dostępowego
27. Adres IP punktu dostępowego
28. Status punktu dostępowego
29. Przypisanie do lokalizacji
30. Informacje o kanałach pracy poszczególnych interfejsów radiowych
31. Informacje o liczbie klientów na poszczególnych interfejsach radiowych
32. Informacje o aktualnej mocy ustawionej na poszczególnych interfejsach radiowych
33. Informacji o szerokości kanału ustawionej na poszczególnych interfejsach radiowych
34. Informacji o statusie portów Ethernet i ewentualnej konfiguracji połączeń Link Aggregation na portach Etherent punktów dostępwowych
35. Informacji o poziomie szumu dla poszczególnych interfejsów radiowych
36. Kontroler musi zapewniać możliwość filtracji prezentowanych informacji o punktach dostępowych na podstawie dowolnych parametrów
37. Kontroler musi zapewniać możliwość konfiguracji sieci bezprzewodowych, ich przydziału do grup punktów dostępowych, a następnie do lokalizacji
38. Kontroler musi zapewniać automatyczne wykrywanie i konfigurowanie nowych punktów dostępowych
39. Kontroler musi być zarządzany przez SNMPv1/v2/v3 oraz SSHv2.
40. Kontroler musi obsługiwać RADIUS authentication oraz RADIUS accounting.
41. Kontroler musi zapewniać obsługę: 802.11i, WPA, WPA2, TKIP oraz AES, WPA3
42. Kontroler musi zapewniać obsługę rozwiązania OWE (Opportunistic Wireless Encryption) zapewniającego bezpieczeństwo w sieciach „otwartych”
43. Kontroler musi zapewniać obsługę IEEE 802.1x oraz autentykację: EAP-TLS, EAP-TTLS, PEAP, EAP-MD5 oraz EAP-SIM.
44. Obsługa mechanizmów roaming oraz handover (wstępne uwierzytelnienie, OKC)
45. Kontroler musi zapewniać obsługę najnowszych standardów realizacji roamingu IEEE 802.11r
46. Kontroler musi zapewniać obsługę Neighbor Report w ramach standardu IEEE 802.11k
47. Kontroler musi zapewniać obsługę mechanizmów Roaming Assist zgodnych ze standardem IEEE 802.11v
48. Kontroler musi zapewniać obsługę mechanizmów IEEE 802.11w
49. Kontroler musi zapewniać przesyłanie danych z sieci WLAN do sieci przewodowej w następujących architekturach:
50. bridging na kontrolerze – kontroler zapewnia przełączanie ruchu z sieci bezprzewodowej do wskazanej sieci wirtualnej przewodowej dołączonej do kontrolera
51. bridging na punkcie dostępowym – w tym trybie ruch z sieci bezprzewodowej jest kierowany bezpośrednio do wskazanej sieci wirtualnej przyłączonej bezpośrednio do punktu dostępowego
52. bridging na punkcie dostępowym wraz z sygnalizacją niezbędnych sieci VLAN z wykorzystaniem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB)
53. bridging na punkcie dostępowym z zapewnieniem tunelowania ruchu poprzez VxLAN
54. Kontroler bezprzewodowy musi zapewniać możliwość ustawiania następujących parametrów w ramach każdej sesji klienckiej:
55. indywidualne raguły filtrowania ruchu
56. przypisanie sieci VLAN
57. QoS
58. ograniczenia transmisji wejściowej i wyjściowej
59. wyboru topologii (bridging na kontrolerze, bridging na punkcie dostępowym, tunel VxLAN, IEEE 802.1Qcj)
60. Kontroler musi zapewniać obsługę konfiguracji punktów dostępowych w trybie Client Bridge, który będzie wykorzystywał punkt dostępowych jako klienta do sieci bezprzewodowej przy wykorzystaniu jednego z interfejsów radiowych (2.4 GHz lub 5 GHz) jednocześnie udostępniając obydwa interfejsy radiowe dla klientów bezprzewodowych oraz dostępne interfejsy Ethernet do przyłączenia urządzeń nieposiadających interfejsu bezprzewodowego do sieci bezprzewodowej
61. Kontroler musi zapewniać możliwość centralnej konfiguracji przyłączenia punktów dostępowych do infrastruktury sieciowej zabezpieczonej przez IEEE 802.1x i protokoły PEAP oraz EAP-TLS (IEEE 802.1x supplicant na porcie Ethernet punktu dostępowego)
62. Kontroler musi zapewniać możliwość konfiguracji rozwiązania Mesh
63. Kontroler musi zapewniać obsługę standardu Hotspot 2.0
64. Kontroler musi zapewniać współpracę z systemem Eduroam
65. Kontroler musi zapewniać obsługę Captive Portal pozwalającego na obsługę gości jak i uwierzytelnianie klientów bezprzewodowych z wykorzystaniem Captive Portal – np. nieposiadających suplikanta IEEE 802.1x
66. Kontroler musi zapewniać możliwość rejestracji gości w oparciu o portal www znajdujący się na kontrolerze.
67. Portal rejestracji gości musi zapewniać możliwość konfiguracji danych niezbędnych dla rejestracji np.: Imię, Nazwisko, email, numer telefonu, PESEL, nr. Dowodu itp.
68. Portal rejestracji gości musi zapewniać możliwość stworzenia i akceptacji regulaminu przez rejestrujących się gości
69. Kontroler musi zapewniać przynajmniej podstawową konfigurację wyglądu Captive Portal – zmiana kolorów itp.
70. 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.
71. Captive Portal musi zapewniać wsparcie min. języka polskiego, angielskiego i niemieckiego.
72. Captive Portal musi zapewniać obsługę urządzeń mobilnych
73. Kontroler musi zapewniać rejestrację gości z wykorzystaniem portali społecznościowych np. Facebook, Google, itp
74. Kontroler musi zapewniać możliwość automatycznej, centralnej aktualizacji oprogramowania punktów dostępowych zaadoptowanych do kontrolera.
75. Kontroler musi zapewniać możliwość konfiguracji blokowania ruchu pomiędzy klientami sieci bezprzewodowej.
76. Kontroler musi zapewniać autoryzację użytkowników IEEE 802.1x w oparciu o zewnętrzny serwer RADIUS z możliwością definicji różnych serwerów RADIUS dla różnych identyfikatorów SSID
77. Kontroler musi zapewniać przydzielanie klientów do wskazanych sieci wirtualnych na podstawie informacji przesyłanej z serwera RADIUS zgodnie z RFC3580
78. Kontroler musi zapewniać możliwość uwierzytelniania z wykorzystaniem Microsoft Active Directory
79. Kontroler musi zapewniać możliwość przydzielania do sieci VLAN na podstawie przynależności klientów bezprzewodowych do grup użytkowników zdefiniowanych w LDAP
80. 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.
81. Powyższe Polityki muszą być spójne z Politykami implementowanymi na przełącznikach znajdujących się w piętrowych punktach dystrybucyjnych i muszą być konfigurowane centralnie z oprogramowania zarządzającego
82. Kontroler musi zapewniać konfigurację roamingu pomiędzy punktami dostępowymi.
83. Kontroler musi zapewniać konfigurację oszczędzania energii UAPSD (Unscheduled Automatic Power Save Delivery).
84. Kontroler musi obsługiwać QBSS (informacja o zbyt dużym obciążeniu zostanie przekazana klientowi dla obsługi inteligentnego roamingu)
85. 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.
86. Kontroler musi obsługiwać funkcjonalność CAC (Call Admission Control), pozwalającą na sprawdzenie czy zestawienie nowego połączenia telefonii VoIP nie wpłynie na jakość dotychczasowych połączeń.
87. Kontroler musi zapewniać obsługę preferencji pasma polegającą na automatycznym przenoszeniu klientów na pasmo 5 GHz.
88. Kontroler musi zapewniać możliwość uruchamianie sieci bezprzewodowych wg. skonfigurowanego planu bazującego na kalendarzu bez konieczności angażowania administratora.
89. Jednorazowe włączenie wskazanej sieci bezprzewodowej – od dnia i godziny do dnia i godziny – przykładowo na potrzeby organizowanej konferencji
90. Codzienne włączanie wskazanej sieci bezprzewodowej – od godziny do godziny – przykładowo wyłączanie sieci bezprzewodowej w godzinach zamknięcia budynku
91. Włączanie wskazanej sieci bezprzewodowej w konkretne dni tygodnia – od godziny do godziny – przykładowo włączanie sieci bezprzewodowej we wtorki i czwartki w konkretnych godzinach na potrzeby np. konkretnych wykładów
92. Powyższe mechanizmy muszą zapewniać podgląd listy poszczególnych zdarzeń oraz podgląd zdarzeń w kalendarzu dostępnym poprzez interfejs graficzny kontrolera
93. Kontroler musi zapewniać interfejs REST API dla integracji z rozwiązaniami firm trzecich lub własnymi systemami UJ.
94. Kontroler musi zapewniać instalację min. dwóch obrazów firmware dla kontrolera
95. Kontroler musi zapewniać realizację backupów konfiguracji

1. **Wymagania na punkty bezprzewodowe WiFi6**

1. Punkt dostępowy dwuradiowy do zastosowań wewnątrz-budynkowych z wbudowanymi antenami dookólnymi
2. Punkt dostępowy musi być wyposażony w min. 1 port Ethernet 10/100/1000 Mbps Base-T RJ-45 z możliwością zasilenia punktu dostępowego przez skrętkę.
3. Punkt dostępowy musi być wyposażony w interfejs USB
4. Punkt dostępowy musi zapewniać wsparcie dla standardów 802.11a/b/g/n/ac oraz Wi-Fi 6 (802.11ax)
5. Punkt dostępowy musi być wyposażony w min. 2 interfejsy radiowe:
6. 2,4GHz ze wsparciem dla technologii MIMO 2x2:2,
7. 5GHz ze wsparciem dla technologii MIMO 2x2:2,
8. Punkt dostępowy musi wspierać następujący tryby pracy interfejsów radiowych:
9. 2.4GHz / 5 GHz
10. 5 GHz / 5GHz (Dual 5 GHz)
11. Praca jako sensor dla systemu IPS/IDS
12. Punkt dostępowy musi być wyposażony w moduł radiowy służący do obsługi standardów BLE i IEEE 802.15.4
13. Punkt dostępowy musi być wyposażony w min. 5 anten wewnętrznych w tym jedna dedykowana do obsługi standardów BLE i IEEE 802.15.4
14. Punkt dostępowy musi mieć możliwość zasilania z wykorzystaniem technologii Power-over-Ethernet (PoE) w standardzie IEEE 802.3af – max. 15.4 W
15. Punkt dostępowy musi mieć możliwość pracy w temperaturze z zakresu od 0°C do 40°C
16. Punkty dostępowe muszą obsługiwać IP QoS w środowisku przewodowym i bezprzewodowym. Rozróżnianie pakietów musi być realizowane dla przychodzących i wychodzących pakietów z sieci bezprzewodowej, w oparciu o DiffServ, IP ToS oraz IP Precedence
17. Punkty dostępowe muszą obsługiwać wsparcie dla protokołu IEEE 802.1p prioritization
18. Punkty dostępowe musza obsługiwać protokoł 802.11e, w tym WMM oraz U-APSD
19. Punkty dostępowe musza obsługiwać mechanizmów roaming oraz handover (wstępne uwierzytelnienie, OKC)
20. Punkt dostępowy musi obsługiwać mechanizm szybkiego roamingu IEEE 802.11r
21. Punkt dostępowy musi obsługiwać mechanizm Neighbour Report IEEE 802.11k
22. Punkt dostepowy musi obsługiwać standard IEEE 802.11v
23. Punkt dostępowy musi obsługiwać do 16 SSID (8 na częstotliwość radiową)
24. Punkt dostępowy musi obsługiwać mechanizm RADIUS Authentication & Accounting
25. Punkt dostępowy musi obsługiwać logowanie użytkowników z wykorzystaniem IEEE 802.1X oraz metodami: EAP-TLS, EAP-TTLS, PEAP oraz EAP-SIM
26. Punkt dostępowy musi obsługiwać mechanizmu MAC Address Authentication
27. Punkt dostępowy musi zapewniać izolację klientów na poziomie L2,
28. Punkt dostępowy musi zapewniać wsparcie dla standardu WPA3
29. Punkt dostępowy musi zapewniać wsparcie dla mechanizmów IEEE 802.11i, WPA2 oraz WPA, przy zastosowaniu algorytmów szyfracji Advanced Encryption Standard (AES) oraz Temporal Key Integrity Protocol (TKIP)
30. Obsługa technologii SU-MIMO oraz MU-MIMO dla standardu WiFi 6 (802.11ax)
31. Musi mieć możliwość zapewnienia równego czasu antenowego (Airtime) dla wszystkich klientów w środowiskach, w których wspólnie występują technologie 802.11a/b/g, 802.11n, 802.11ac oraz 802.11ax.

Podział strony

1. **System zarządzający**

1. 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.
2. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux oraz jaka aplikacja dedykowana dla systemu wirtualizacyjnego.
3. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
4. Dostarczenie oprogramowanie zarządzające musi być obsługiwanego ze standardowej przeglądarki www bez konieczności instalacji dodatkowego klienta lub wymagania instalacji dodatkowego oprogramowania jak np. Java
5. Aplikacja zarządzająca musi obsługiwać minimum 2500 urządzeń (adresów IP zarządzanych przez SNMP) przy czym oprogramowanie musi być dostarczone z licencjami niezbędnymi do zarządzania dostarczonych urządzeń.
6. Aplikacja zarządzająca musi zapewniać możliwość zarządzania dowolnymi urządzeniami posiadającymi obsługę protokołu SNMP i/lub dostęp poprzez CLI (Telnet i/lub SSH)
7. Aplikacja zarządzająca musi zapewniać możliwość jednoczesnego podłączenia się do platformy zarządzającej min. 10 użytkowników. W skład tych użytkowników będą wchodzić administratorzy sieci oraz osoby wsparcia technicznego klientów – HelpDesk
8. Aplikacja zarządzająca musi mieć możliwość definiowania grup użytkowników i definicji praw dostęp do różnych funkcji oprogramowania. Aplikacja musi zapewniać możliwość przydziału użytkowników systemu do różnych grup użytkowników
9. Aplikacja zarządzająca musi mieć możliwość integracji uwierzytelniania i autoryzacji użytkowników za pomocą LDAP i/lub Radius.
10. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
11. Aplikacja zarządzająca musi zezwalać na zarządzanie urządzeniami z wykorzystaniem protokołów SNMPv1, SNMPv2c, SNMPv3. SNMPv3 musi zapewniać uwierzytelnianie za pomocą protokołów MD5 oraz SHA, szyfrowanie za pomocą protokołów DES oraz AES.
12. Aplikacja musi pozwalać na tworzenie profili dostępu do urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu. Profil musi zawierać konfigurację SNMP dla danego urządzenia z podziałem na pełny dostęp, dostęp dla zapisu i odczytu oraz dostęp tylko do odczytu.
13. Dodatkowo profil dostępu do urządzeń musi zawierać możliwość konfiguracji dostępu do urządzenia z wykorzystaniem CLI – np. poprzez Telnet lub SSH.
14. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
15. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
16. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
17. Aplikacja musi zapewniać możliwość konfiguracji widoków zawierających wskazane obiekty SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych. Przykładowo możliwość włączania/wyłączania portów, konfiguracji opisu portu (alias), włączenie/wyłączenie IEEE 802.1x, prezentację obciążenia portów PoE+ i inne dostępne w SNMP MIB OID dowolnego producenta.
18. Aplikacja musi zezwalać na modyfikację wyżej wymienionych obiektów SNMP MIB OID jeśli są to obiekty pozwalające na zapis i odczyt informacji.
19. Aplikacja musi posiadać wbudowany Syslog serwer pozwalający na gromadzenie logów przesyłanych przez zarządzane urządzenia.
20. Aplikacja musi posiadać możliwość konfiguracji Alarmów w reakcji na przychodzące trapy SNMP lub informacje z Syslog.
21. Alarmy muszą zapewniać możliwość wysłania emaila, wysłania trapu SNMP do innego systemu zarządzającego lub systemu automatyzacji, wpisu do Syslog lub uruchomienia skryptu.
22. Aplikacja zarządzająca musi zapewniać możliwość tworzenia skryptów CLI dla automatyzacji często wykonywanych zadań na zarządzanych urządzeniach. Skrypty muszą zapewniać możliwość wydawania komend CLI do wskazanych urządzeń lub grup urządzeń.
23. Aplikacja zarządzająca musi zapewniać możliwość tworzenia prostych skryptów CLI nie wymagających od administratora wiedzy programistycznej jak również bardziej zaawansowanych skryptów z wykorzystaniem TCL i Python.
24. Aplikacja zarządzająca musi w ramach powyższych skryptów zapewniać mechanizmy pozwalające na uzyskanie informacji z systemów firm trzecich z wykorzystaniem REST API
25. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
26. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
27. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń.
28. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
29. Lokalizacji urządzeń np. poszczególne lokalizacje, budynki, piętra itp.
30. Wizualizacja sieci musi zapewniać możliwość podłożenia rysunku kampusu lub piętra
31. Połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem numerów portów po obydwu stronach łącza
32. Połączeń Link Aggregation
33. Wizualizacji skonfigurowanych sieci VLAN na poszczególnych urządzeniach
34. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
35. adres IP urządzenia
36. adresu MAC urządzenia
37. nazwy urządzenia
38. wersji oprogramowania
39. wersji bootrom
40. lokalizacji urządzenia
41. danych kontaktowych administratora
42. numeru seryjnego
43. dodatkowych pól konfigurowanych przez użytkownika pozwalających na skonfigurowanie np. numerów inwentarzowych
44. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
45. możliwość automatycznej periodycznej (np. codziennie, co tydzień) realizacji backup’u konfiguracji urządzeń o wskazanym czasie (np. o 01:00).
46. możliwość odtworzenia wskazanej konfiguracji urządzenia
47. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
48. możliwość porównywania różnic w ramach jednego urządzania z różnych backup’ów konfiguracji oraz w ramach różnych urządzeń.
49. możliwość obsługi urządzeń sieciowych różnych producentów
50. 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 zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych różnych producentów (przy założeniu dostępu SSH/Telnet).
51. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
52. Aplikacja musi zapewniać możliwość tworzenia profili bezpieczeństwa, które zawierają konfigurację sieci VLAN, ACL, QoS i mogą być przypisywane statycznie do portów przełączników sieciowych.
53. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
54. 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).
55. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
56. generowanie raportów
57. System zarządzający musi mieć wbudowane API do komunikacji z systemami firm trzecich.
58. System zarządzania musi być objęty 3 letnim wsparciem serwisowym producenta i musi zapewniać również dostęp do poprawek oraz nowych wersji oprogramowania oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia technicznego przez telefon, e-mail lub stronę www trybie 24x7x365 przez okres co najmniej 3 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowanego partnera serwisowego.

1. **System kontroli dostępu**

1. System kontroli dostępu musi zapobiegać przed nieautoryzowanym dostępem użytkowników lub urządzeń do sieci LAN oraz sieci WLAN. Dodatkowo systemu musi zapewniać kontrolę dostępu do zarządzania urządzeń sieciowych poprzez Telnet, SSH, CLI
2. System kontroli dostępu musi zapewniać możliwość instalacji wielu serwerów fizycznych lub wirtualnych zapewniających uwierzytelnianie i autoryzację użytkowników w sieci przy jednoczesnej centralnej konfiguracji wszystkich serwerów. Jeśli liczba serwerów kontroli dostępu jest osobno licencjonowana to wymagane jest dostarczenie licencji na min. 2 instancje
3. System kontroli dostępu musi zapewniać możliwość dodawania urządzeń (np. przełącznik, kontroler bezprzewodowy), które będą korzystały z systemu kontroli dostępu i pozwolić na konfigurację serwerów, z których będzie korzystać konkretne urządzenie. Dla każdego dodawanego urządzenia musi być zapewniona możliwość konfiguracji zestawu atrybutów RADIUS wysyłanych jako odpowiedź z autoryzacją oraz mechanizm realizacji reauthentykacji CoA.
4. System kontroli dostępu musi zapewniać możliwość reauthentykacji dla poszczególnych urządzeń z wykorzystaniem standardowego CoA RFC 3576/5176 lub z wykorzystaniem SNMP
5. System kontroli dostępu musi zapewniać obsługę RADIUS Accounting, który pozwoli na informowanie systemu kontroli dostępu o stanie dołączonego urządzenia – podłączone/niepodłączone.
6. System kontroli dostępu musi zapewniać uwierzytelnianie dołączonych do przełączników sieciowych lub bezprzewodowych punktów dostępowych z wykorzystaniem IEEE 802.1x oraz MAC Authentication.
7. System kontroli dostępu w ramach IEEE 802.1x musi zapewniać możliwość wykorzystywania następujących protokołów uwierzytelniania:
8. EAP-TLS
9. EAP-TTLS
10. PEAP
11. EAP-MD5
12. PAP
13. CHAP
14. MS-CHAP
15. System kontroli dostępu musi zapewniać możliwość wizualizacji dołączanych systemów końcowych do sieci LAN i WLAN z możliwością prezentacji następujących parametrów:
16. Stan systemu końcowego – np. włączony/wyłączony, błąd uwierzytelniania bądź autoryzacji
17. MAC adres systemu końcowego
18. Adres IP systemu końcowego
19. Nazwa systemu końcowego – Hostname
20. Typ systemu końcowego wraz z systemem operacyjnym – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows, MAC OS, IOS, Android
21. Nazwa urządzenia, do którego dołączony jest system końcowy – może to być np. nazwa przełącznika sieciowego lub nazwa punktu dostępowego w przypadku sieci bezprzewodowej
22. Adres IP urządzenia, do którego dołączony jest system końcowy –adres IP przełącznika sieciowego lub adres IP kontrolera bezprzewodowego, który przeprowadził uwierzytelnienie i autoryzację.
23. Identyfikację portu, do którego dołączony jest system końcowy – identyfikacja sieci bezprzewodowej (SSID) lub portu przełącznika sieciowego.
24. Typ uwierzytelniania systemu końcowego np. MAC authentication, IEEE 802.1x – EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, Kerberos snooping itp.
25. Nazwa przydzielonego profilu bezpieczeństwa.
26. System kontroli dostępu musi zapewniać możliwość wybrania z powyższej wizualizacji dowolnego systemu końcowego i wykonanie na nim następujących operacji:
27. wymuszenie ponownego uwierzytelnienia
28. sprawdzenie dostępności urządzenia z wykorzystaniem mechanizmu „ping”
29. otworzenie okna terminala do urządzenia, które zrealizowało uwierzytelnienie – przełącznik, kontroler bezprzewodowy
30. otworzenie zarządzania http/https do urządzenia, które zrealizowało uwierzytelnienie – przełącznik, kontroler bezprzewodowy
31. przeniesienie systemu końcowego do wcześniej stworzonej grupy (np. wskazanie wykrytej drukarki i przeniesienie jej do grupy drukarek)
32. symulację procesu uwierzytelniania i autoryzacji – wizualizacja jak proces przebiegał i jakie warunki zadziałały dla danego systemu końcowego
33. usunięcie systemu końcowego z bazy danych
34. otworzenie mapy wskazującej lokalizację systemu końcowego (w przypadku przełącznika ma być wskazany przełącznik, gdzie nastąpiło uwierzytelnienie, a w przypadku sieci bezprzewodowej powinna być wskazana lokalizacja uwierzytelnionego urządzenia na mapie z wykorzystaniem triangulacji
35. System kontroli dostępu musi zapewniać przechowywanie historii uwierzytelnionych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana profilu bezpieczeństwa itp.
36. System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
37. 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
38. 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.
39. System kontroli dostępu do sieci musi posiadać informacje podsumowujące zawierające:
40. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
41. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
42. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
43. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
44. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
45. System kontroli dostępu do sieci, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 3000 urządzeń klienckich (adresów MAC).
46. System zarządzania musi być objęty 3 letnim wsparciem serwisowym producenta i musi zapewniać również dostęp do poprawek oraz nowych wersji oprogramowania oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia technicznego przez telefon, e-mail lub stronę www trybie 24x7x365 przez okres co najmniej 3 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowanego partnera serwisowego.
47. System zarządzania musi zapewniać wizualizację analityki aplikacji działających w sieci LAN
48. Poszczególne dodatkowe komponenty systemu zarządzania powinny być zintegrowane z podstawowym systemem zarządzającym i posiadać wspólny interfejs zarządzania www. W przypadku zaproponowania odrębnych systemów konieczne jest zapewnienie pojedynczego logowania do wszystkich systemów z wykorzystaniem Single Sign-On.

1. **System analizy aplikacji działających w sieci LAN i WLAN**

1. System ma za zadanie wykrywanie i prezentowanie informacji o aplikacjach wykorzystywanych przez użytkowników sieci przewodowej oraz bezprzewodowej
2. System musi współpracować z dostarczonymi przełącznikami oraz punktami dostępowymi, które muszą dostarczać niezbędne informacje na potrzeby wykrywania aplikacji działających w sieci.
3. System analizy aplikacji musi zapewniać możliwość wykrywania aplikacji działających w sieci LAN i WLAN na podstawie dostarczonych wraz z systemem sygnatur ruchu sieciowego. Liczba sygnatur ruchu sieciowego nie może być mniejsza niż kilkanaście tysięcy i musi pozwalać na wykrywanie kilku tysięcy aplikacji
4. System analizy aplikacji musi zapewniać możliwość tworzenia własnych sygnatur wykrywania aplikacji na wartswie 7
5. System analizy aplikacji musi zapewniać możliwość tworzenia własnych sygnatur również poprzez definiowanie portu TCP/UDP, zakresu portów TCP/UDP, adresu IP serwera, zakresu adresów IP serwera oraz HTTP URL
6. Wykrywanie aplikacji musi się odbywać do warstwy 7 modelu OSI pozwalając na rozróżnianie aplikacji działających z wykorzystaniem tego samego portu TCP/UDP.
7. System musi zapewniać możliwość pomiaru czasu odpowiedzi sieci oraz czasu odpowiedzi aplikacji, co pozwoli na jednoznaczne określenie miejsca występujących problemów – sieć LAN, WLAN, czy sama aplikacja lub serwer, na którym aplikacja jest uruchomiona
8. System analizy aplikacji musi zapewniać możliwość monitorowania krytycznych dla pracy sieci aplikacji takich jak: DNS, DHCP, Radius, Kerberos, LDAP. Odbiegające od normy lub przekroczenie zdefiniowanych czasów odpowiedzi aplikacji musi być raportowane w postaci alarmów. Obsługa alarmów musi być zapewniona zgodnie z wymaganiami opisanymi dla platformy zarządzającej.
9. System analizy aplikacji musi zapewniać możliwość śledzenia wybranych lub własnych zdefiniowanych aplikacji.
10. System musi zapewniać możliwość tworzenia raportu zawierającego najgorzej działające aplikacje w sieci lub jej fragmencie (poprzez podanie lokalizacji). Identyfikacja najgorzej działającej aplikacji powinna się odbywać poprzez analizę czasów odpowiedzi sieci i czasów odpowiedzi aplikacji
11. System musi zapewniać możliwość uzyskania informacji o wykorzystaniu sieci przez poszczególne aplikacje w określonym czasie z uwzględnieniem.
12. Zajmowanego pasma
13. Liczby przepływów (flow)
14. Liczby klientów
15. System musi zapewniać możliwość przeszukiwania gromadzonych informacji i wyświetlania raportów z możliwością filtrowania informacji na podstawie:
16. Lokalizacji
17. Grupy aplikacji – np. Mail, Cloud Storage, Social Networking, VPN itp.
18. Wskazanej konkretnej aplikacji – np. Facebook, Google Mail, Google Calendar, Microsoft Office 365
19. Rodziny urządzeń klienckich – np. Windows, Android, Linux,
20. Zalogowanego klienta – przykładowo wszystkie aplikacje wykorzystywane przez użytkownika Jan Kowalski (nazwa użytkownika wynika z loginu użytkownika)
21. Wyszukiwane powyżej dane muszą mieć możliwość prezentacji w formie tabelarycznej lub w postaci wykresów
22. System musi posiadać mechanizmy do automatycznego, periodycznego wysyłania raportów pod wskazany adres email.
23. System musi posiadać możliwość wyświetlenia wszystkich przepływów (flow) otrzymanych z urządzeń sieciowych ze wskazaniem adresów źródłowego i docelowego, aplikacji, grupy aplikacji, czasu odpowiedzi sieci i czasu odpowiedzi aplikacji, lokalizacji oraz nazwy użytkownika pochodzącej z systemu kontroli dostępu.

Podział strony

1. **System Firewall**

1. **Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i  bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.
1. **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
6. **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 8 gniazdami SFP+ 10 Gbps.
* 2 gniazdami QSFP+ 40 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie 2xAC.
4. **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 480 tyś. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 45 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 25 Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 46 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 12 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 10 Gbps.
10. **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych  - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami  - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system
14. **Polityki, Firewall**

1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
* Amazon Web Services (AWS).
* Microsoft Azure
* Cisco ACI.
* Google Cloud Platform (GCP).
* Nuage Networks VSP.
* OpenStack.
* VMware vCenter (ESXi).
* VMware NSX.
* VMware NSX.Nutanix
* VMware NSX.IBM Cloud

1. **Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman  grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* Pracę w trybie Portal  - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
1. **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
1. **Funkcje SD-WAN**

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
3. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec.
4. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.
5. **Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma,  oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
4. **Ochrona przed malware**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
7. **Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
6. **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL  pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
9. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla servisów youtube, vimeo.
10. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.
11. **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
4. **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami  centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami  centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. **Logowanie**

1. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.
4. **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.
1. **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

1. **Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. **Opisy do wymagań ogólnych**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

1. **Zakres wdrożenia i lista prac do wykonania**

1. *Dostawa urządzeń:*
2. *Przełączbit niki Giga Ethernet dla piętrowych punktów dystrybucyjnych*
3. *Przełączniki 10 Gigabit Ethernet dla piętrowych punktów dystrybucyjnych*
4. *Punkty dostępowe*
5. *System firewall (UTM)*
6. *Wykonanie modelu predykcyjnego sieci bezprzewodowej w oprogramowaniu umożliwiającym kompletny eksport a następnie import wykonanych planów do oprogramowania kontrolera sieci bezprzewodowej, zamawiający sugeruje oprogramowanie Ekahau lub AirMagnet ze względu na znajomość tego oprogramowania.*
7. *Wykonanie dokumentacji powdrożeniowej obejmującej co najmniej*
8. *Opisy i rysunki zainstalowanych urządzeń*
9. *Dokumentację okablowania strukturalnego dla “IDF Sekretariat” oraz bezprzewodowych punktów dostępowych naniesioną na plany budynku*
10. *Opis konfiguracji softwarowej*
11. *Mapę sieci wraz z opisem połączeń fizycznych*
12. *Mapę zasięgów sieci bezprzewodowej wraz z raportem*
13. *Instalacja bezprzewodowych punktów dostępowych. Doprowadzenie okablowania strukturalnego do zaprojektowanych miejsc instalacji punktów dostępowych.*
14. *Weryfikacja przygotowanego modelu predykcyjnego w rzeczywistości i wprowadzenie ewentualnych modyfikacji poziomów sygnału w celu zapewnienia planowanego zasięgu*
15. *Instalacja urządzeń sieciowych w Centralnym Punkcie Dystrybucyjnym oraz wszystkich piętrowych punktach dostępowych. Instalacja musi być uzgodniona z Zamawiającym i powinna jak najmniej wpływać na działanie aktualnej sieci.*
16. *Dostarczenie odpowiedniej długości patchcordów, (nie dłuższych niż 120% długości wymaganego odcinaka pomiędzy patchpanelem a przełącznikiem) w ilości opisanej w punkcie 2.1 dot. Ilości portów.*
17. *Patchcordy użyte do krosowania połączeń z bezprzewodowymi punktami dostępowymi powinny być innego koloru niż zielony (zarezerwowoany dla połączeń telefonicznych) i użyty do połączeń portów klienckich.*
18. *Skrosowanie wszystkich wymaganych połączeniem portów wskazanych przez zamawiającego i ułożenie kabli w prowadnicach. W ilości nie mniejszej niż opisanej w pkt. 2.1 dot. ilości portów w poszczególnych punktach dystrybucyjnych.*
19. *Instalacja oprogramowania zarządzającego, systemu kontroli dostępu oraz analityki aplikacji na systemie wirtualizacyjnym Zamawiającego wyspecyfikowanym w* pkt. 4 pt. Opis systemu wirtualizacyjnego
20. *Konfiguracja systemu zarządzającego*
21. *Dodanie wszystkich urządzeń sieciowych (przełączniki, kontrolery bezprzewodowe, klaster firewall) do oprogramowania zarządzającego – konfiguracja profili SNMP i dostępu SSH w celu bezpośredniego dostępu do CLI i ewentualnego wykonywania skryptów*
22. *Konfiguracja automatycznej archiwizacji konfiguracji urządzeń sieciowych*
23. *Konfiguracja systemu kontroli dostępu*
24. *Uruchomienie uwierzytelniania IEEE 802.1x oraz MAC Authentication na przełącznikach piętrowych Gigabit Ethernet*
25. *Uruchomienie integracji kontroli poświadczeń użytkowników z Centralnym Systemem zarządzania tożsamością z wykorzystaniem protokołów OpenId Connect, SAML 2, ew. LDAP*
26. *Uruchomienie kontroli poświadczeń użytkowników w oparciu o wewnętrzne bazy użytkowników.*
27. *Konfiguracja uwierzytelniania punktów dostępowych dołączonych do przełączników Gigabit Ethernet w piętrowych punktach dystrybucyjnych.*
28. *Konfiguracja urządzeń obejmująca co najmniej:*
29. *Stworzenia sieci VLAN dla zarządzania urządzeń aktywnych (przełączników)*
30. *Adresacja urządzeń aktywnych*
31. *Stworzenie wydzielonej sieci VLAN dla zarządzania punktów dostępowych*
32. *Konfiguracja routingu*
33. *Stworzenie i konfiguracja adresacji IP dla grup użytkowników (adresacja wew. i publiczna)*
34. *Konfiguracja polityk bezpieczeństwa dla grup użytkowników*
35. *Konfiguracja sieci wirtualnych VLAN dla różnych grup użytkowników*
36. *Instalacja i konfiguracja Windows 2019 Domain Controler lub tożsamego np. Samba w wersji 4*
37. *Konfiguracja klastra UTM obejmująca co najmniej:*
38. *Konfiguracje na serwerze wirtualnym (dostarczonym przez Zamawiającego) serwera DNS do obsługi stref DNS*
39. *Wdrożenie domeny z certyfikatem wildcard (dostarczonym przez Zamawiajacego)*
40. *Konfiguracje NAT, dla min. kilkunastu grup i działów (DMZ, drukarki, goście, Policy-Based NAT)*
41. *Konfiguracje reguł wejściowych i wyjściowych oraz interfejsów*
42. *Konfiguracje serwera DHCP*
43. *Konfiguracje VPN i integracje z centralnym Systemem zarządzania tożsamością z wykorzystaniem protokołów OpenId Connect, SAML 2*
44. *Przygotowanie plików konfiguracyjnych zawierających dane do połączenia z VPN pozwalających na łatwy import po stronie oprogramowania klienckiego.*
45. *Konfiguracja funkcjonalności “SSL VPN web portal” - jeżeli producent wymaga odpowiednich licencji musi ona być dostarczona wraz z urządzeniem.*
46. *Przeprowadzenie testów symulujących awarię i przełączenie łączy z podstawowych na zapasowe*
47. *Wdrożenie musi być wykonane zgodnie z wymaganiami normy ISO 27001. Wymagane jest aby oferent posiadał certyfikat ISO 27001.*
48. *Konfiguracja sieci bezprzewodowej zgodnie z wytycznymi Zamawiającego w tym co najmniej*
49. *Konfiguracja adresacji*
50. *Konfiguracja profili radiowych*
51. *Konfiguracja polityk bezpieczeństwa*
52. *Konfiguracja autentykacji z wykorzystaniem protokołów OpenId Connect, SAML 2 oraz Integracja z systemem Uniwersyteckim UJ\_WIFI oraz z systemem*<https://www.eduroam.pl/>*(w tym integracja z systemem uwierzytelniania RADIUS)*
53. *Konfiguracja Captive Portal*
54. *Szkolenie administratorów z zainstalowanych systemów w wymiarze min. 30 godzin w miejscu instalacji, lub zdalnie jeżeli będzie to możliwe.*
55. *Zamawiający wymaga asysty powdrożeniowej w wymiarze 100  godzin w ciągu roku od daty zakończenia wdrożenia. Wymagane jest, aby asysta była realizowana przez certyfikowanych inżynierów oferenta. Ze względów bezpieczeństwa systemów teleinformatycznych asysta będzie realizowana na miejscu u Zamawiającego (w przypadku zmiany obostrzeń epidemiologicznych sposób realizacji zostanie ustalony przez Zamawiającego i Oferenta)*

1. **Opis systemu wirtualizacyjnego.**

 Poniższy opis zawiera informację dotyczącą posiadanych przez Zamawiającego urządzeń możliwych do wykorzystania do wirtualizacji niezbędnych systemów takich jak:

* Oprogramowanie zarządzające
* System kontroli dostępu
* System analizy aplikacji
* Kontrolery bezprzewodowe
* Itp.

 Na powyższe potrzeby mogą być wykorzystane dwa serwery tworzące klaster. Do stworzenia klastra mogą być wykorzystane wszystkie poniższe urządzenia. Klaster musi być zainstalowany i uruchomiony przez Oferenta.

Lista posiadanych urządzeń:

2x Supermicro CSE-826, 2 x E5-2650, 64GB, HBA 6gbps, 2TB SSD

1. **Wymagania projektu sieci bezprzewodowej.**

 **Wymagania dotyczące projektu sieci bezprzewodowej**

1. Zamawiający, po wcześniejszym umówieniu, udostępni pomieszczenia do przeprowadzenia wizji lokalnej i pomiarów niezbędnych do przeprowadzenia projektu predykcyjnego w oprogramowaniu Ekahau or Air Magnet.
2. Zamawiający posiada również podkłady wszystkich pomieszczeń, które mogą być wykorzystane do projektu
3. Projekt sieci bezprzewodowej należy przeprowadzić przy następujących założeniach:
4. Poziom sygnału do projektu należy przewidzieć na poziomi -65 dBm, a w uzasadnionych przypadkach -70 dBm.
5. Projekt musi obsługiwać sieć bezprzewodową pracującą w paśmie 2.4 GHz oraz w paśmie 5 GHz. Sieć 5 GHz powinna być traktowana jako sieć podstawowa ze względu na liczbę dostępnych nienakładających się kanałów bezprzewodowych
6. Projekt powinien zakładać użycie kanałów 20 lub 40 MHz w zależności od liczby dostępnych kanałów (konieczne jest sprawdzenie dostępności kanałów DFS w danej lokalizacji)
7. Poziomy sygnału ustawione dla punktów dostępowych powinny się zawierać w następujących przedziałach:
8. 7-10 dBm dla 5 GHz
9. 0-7 dBm dla 2.4 GHz
10. Zamawiający wskaże miejsca, w których konieczne będzie zapewnienie obsługi dużej gęstości klientów bezprzewodowych.