WSPiA Rzeszowska Szkoła Wyższa
ul. Cegielniana 14
35-310 Rzeszów
NIP: 795-10-56-506
REGON: 650162512
www.wspia.eu

ZAPYTANIE OFERTOWE NR 8/KON/z045/2021

WARUNKI ZAMÓWIENIA

NA ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI OBEJMUJĄCYCH:

1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;

w ramach projektu pn.:

„NOWY WYMIAR STUDIOWANIA w WSPIA"

WND POWR.03.05.00-00-z045/17, działanie 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego.

Rzeszów, dnia 29 kwietnia 2021 roku

Zatwierdził:
REKTOR
dr hab. prof. WSPiA Jerzy Posłuszny
.....
Podpis

PROJEKT „NOWY WYMIAR STUDIOWANIA W WSPIA"
PROJEKT WSPÓŁFINANSOWANY ZE ŚRODKÓW EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO W RAMACH PROGRAMU OPERACYJNEGO WIEDZA EDUKACJA I ROZWÓJ 2014-2020
PROJEKT NR POWR.03.05.00-00-z045/17

I. Nazwa Zamawiającego:

WSPiA Rzeszowska Szkoła Wyższa z siedzibą w Rzeszowie
ul. Cegielniana 14
35-310 Rzeszów,
NIP: 795-10-56-506,
REGON: 650162512
Telefony kontaktowe: tel.: (17) 867 04 46 w godz.: 8.00-15.00
strona internetowa: www.wspia.eu
- zwana dalej Zamawiającym.

Adres do korespondencji:

WSPiA Rzeszowska Szkoła Wyższa
ul. Cegielniana 14,
35-310 Rzeszów
Budynek „A" I piętro, pokój 2.01.

II. Oznaczenie postępowania:

Nr zapytania ofertowego 8/KON/z045/2021
Wykonawcy powinni we wszystkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.

III. Słownik pojęć użytych w Warunkach zamówienia:

1. **Zamawiający -** WSPiA Rzeszowska Szkoła Wyższa z siedzibą w Rzeszowie.
2. **Wykonawca –** podmiot który realizuje Przedmiot Umowy.
3. **Projekt -** „Nowy wymiar studiowania w WSPiA" – WND POWR.03.05.00-00-z045/17 w ramach działania 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego.
4. **Warunki –** WARUNKI ZAMÓWIENIA NA ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI OBEJMUJĄCYCH:
   1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
   2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;

5. **Zapytanie –** Zapytanie ofertowe 8/KON/z045/2021 obejmujące Warunki zamówienia o których mowa w ust. 4;
6. **Wytyczne** - Wytyczne w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 z dnia 21 grudnia 2020 roku, MIiR/2014-2020/12(5).
7. **System nr 1 –** wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej wraz z ich instalacją i wdrożeniem;
8. **System nr 2** – specjalistyczne oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu, licencje bezterminowe, systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożenia (zgodnie z Umową określoną w ust. 12);
9. **Specyfikacja nr 1** - Specyfikacja Techniczna dotycząca **Systemu nr 1** - wyposażenia sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej wraz z ich instalacją i wdrożeniem;
10. **Specyfikacja nr 2** – Specyfikacja Techniczna dotycząca **Systemu nr 2** - specjalistyczne oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu licencje bezterminowe, systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożenia (zgodnie z Umową określoną w ust. 12);
11. **Zamówienie –** odpłatna Umowa określona w ust. 12 zawarta zgodnie z warunkami wynikającymi z umowy o dofinansowania projektu pomiędzy Zamawiającym, a Wykonawcą dotyczącej realizacji przedmiotu zapytania ofertowego.
12. **Umowa -** Umowa NA ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI OBEJMUJĄCYCH:
    1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
    2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;
13. **IZPO** – Instytucja Zarządzająca Programem Operacyjnym.

IV. <u>Podstawa prawna zamówienia:</u>

Warunki zamówienia uwzględniają procedurę określoną w Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 z dnia 21 grudnia 2020 roku, MIiR/2014-2020/12(5). Do przedmiotowego postępowania nie ma zastosowania ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych.

V. <u>Opis przedmiotu zamówienia:</u>

1. Przedmiotem zamówienia jest:
    1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej obejmującej 232 stanowiska komputerowe wraz z ich instalacją i wdrożeniem.
    2) wdrożenie specjalistycznego oprogramowania do zabezpieczenia komputerów podczas egzaminu - licencje bezterminowe obejmujące 232 stanowiska komputerowe wraz z ich systematycznymi aktualizacjami w okresie 4 lat, licząc od daty wdrożenia (zgodnie z Umową określoną w części III ust. 12 Warunków);

2. Szczegółowy opis przedmiotu zamówienia został zawarty odpowiednio w załącznikach do niniejszych Warunków:
   1) Załącznik nr 1 - Specyfikacja nr 1 - Specyfikacja Techniczna dotycząca Systemu nr 1 - wyposażenia sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej wraz z ich instalacją i wdrożeniem;
   2) Załącznik nr 2 - Specyfikacja nr 2 – Specyfikacja Techniczna dotycząca Systemu nr 2 - specjalistycznego oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu licencje bezterminowe, aktualizowane systematycznie w okresie 4 lat, licząc od daty wdrożenia (zgodnie z Umową określoną w ust 12);

3. Wspólny słownik zamówień:
   48730000-4 - Pakiety oprogramowania zabezpieczającego;
   45314320-0 – Instalowanie okablowania komputerowego
   32420000-3 - Urządzenia sieciowe;

4. Cel przedmiotu zamówienia:
   1) w celu umożliwienia studentom WSPiA zdawania egzaminów w systemie SBS, niezbędne jest wyposażenie posiadanej przez Uczelnię sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej obejmującej 232 stanowiska komputerowe;
   2) w celu zabezpieczenia komputerów podczas zdawania egzaminów w systemie SBS niezbędny jest zakup specjalistycznego oprogramowania, które zostanie zainstalowane na każdym z 232 komputerów. Oprogramowanie to uniemożliwi utworzenie odpowiednich polityk zabezpieczeń, które spowodują, że podczas egzaminu student będzie miał dostęp tylko i wyłącznie do stron Uczelni przeznaczonych do zdawania egzaminów. Natomiast pozostałe strony internetowy oraz zasoby Uczelni z materiałami dydaktycznymi zostaną zablokowane na czas egzaminu. Oprogramowanie zabezpieczające posłuży również do zablokowania dostępu do dysku komputera Studentowi zdającemu egzamin, a także do napędu CD/DVD oraz portów USB;

VI. Miejsce realizacji przedmiotu zamówienia:

WSPiA Rzeszowska Szkoła Wyższa
ul. Cegielniana 14, 35-310 Rzeszów

VII. Termin realizacji Przedmiotu zamówienia:

1. Termin zakończenia realizacji przedmiotu Umowy - do 30 dni licząc od daty zawarcia Umowy.
2. Końcowy termin realizacji przedmiotu Umowy oznacza termin końcowego bezusterkowego jego odbioru.

VIII. <u>Ogólne warunki wykonania zamówienia:</u>

1. System nr 1 musi być wykonany zgodnie ze Specyfikacją nr 1.
2. System nr 2 musi być wykonany zgodnie ze Specyfikacją nr 2.
3. Przedmiot zamówienia (System nr 1, System nr 2) musi być wykonany w sposób zgodny z przepisami prawa polskiego, przepisami prawa Unii Europejskiej oraz niniejszymi Warunkami.
4. Wykonawca w dokumentacji powykonawczej dla każdego z Systemów przedłoży m.in. komplet certyfikatów, aprobaty, instrukcje w języku polskim.
5. Uznaje się, że Wykonawca, przed złożeniem oferty uzyskał wszystkie informacje niezbędne do realizacji przedmiotu zamówienia w tym dotyczące ryzyka, trudności i innych okoliczności, jakie mogą mieć wpływ na treść oferty.
6. Uznaje się, że skalkulowane przez Wykonawcę wynagrodzenie ryczałtowe obejmuje wszelkie koszty i wydatki poniesione przez Wykonawcę w związku z realizacją przedmiotu zamówienia, nawet jeżeli w czasie zawarcia Umowy nie można było przewidzieć rozmiaru lub kosztów prac.

IX. <u>Informacja o przewidywanych zamówieniach:</u>

Zamawiający **nie przewiduje** udzielenia zamówień uzupełniających, wariantowych ani częściowych.

X. <u>Warunki stawiane Wykonawcom oraz opis sposobu dokonywania oceny tych warunków:</u>

1. **O udzielenie zamówienia mogą ubiegać się Wykonawcy którzy:**
   1.1. nie podlegają wykluczeniu z przyczyn określonych w ust. 2;
   1.2. spełniają warunki udziału w postępowaniu określone przez Zamawiającego w ust. 3.

2. **Z postępowania o udzielenie zamówienia wyklucza się:**
   2.1. na mocy **podrozdziału 6.5.2 „Zasada konkurencyjności" pkt 2 lit. a** Wytycznych Wykonawców powiązanym osobowo lub kapitałowo z Zamawiającym (z wyjątkami, o których mowa w powołanym zapisie Wytycznych). Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania pomiędzy Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy, a Wykonawcą polegające w szczególności na:
   1) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
   2) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez IZPO;
   3) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   4) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli;
   5) innym niż wskazane w pkt. 1) - pkt 4) powiązaniu pomiędzy Wykonawcą, a Zamawiającym.

2.2. Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo o którym mowa: w art. 165a, art. 181-188, art. 189a, art. 218-221, art. 228-230a, art. 250a, art. 258, art. 270-309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (j.t. Dz. U. z 2019 r. poz. 676 z późn. zm.).

2.3. Wykonawcę jeżeli urzędującego członka organu zarządzającego lub/i nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplemantariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2.2.

2.4. Wykonawcę, który w wyniku zamierzonych działań lub rażącego niedbalstwa wprowadził Zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów.

2.5. Wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd Zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez Zamawiającego w niniejszym postępowaniu o udzielenie zamówienia.

2.6. Wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienie publiczne na podstawie ustawy z 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (j.t. Dz. U. z 2019 r., poz. `628 z późn. zm.).

2.7. Wykonawcę, w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym przewidziano zaspokojenie wierzycieli przez likwidacje jego majątku lub sąd zarządził likwidację tego majątku lub tego Wykonawcę, którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego.

Wykluczeniu podlega Wykonawca, wobec którego zachodzi co najmniej jedna z ww. przesłanek. Ofertę Wykonawcy wykluczonego z postępowania uznaje się za odrzuconą.

3. **Do postępowania w sprawie udzielenia zamówienia zostaną dopuszczeni Wykonawcy spełniający łącznie następujące warunki:**

3.1. posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania – zgodnie ze złożonym oświadczeniem;

3.2. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie przedmiotu zamówienia we wskazanym terminie - – zgodnie ze złożonym oświadczeniem;

3.3. posiadają niezbędną wiedzę i doświadczenie oraz dysponują odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania zamówienia- – zgodnie ze złożonym oświadczeniem;

3.4. potwierdzą posiadanie niezbędnej wiedzy oraz doświadczenia do należytego wykonania przedmiotu zamówienia przejawiającą się następującym minimalnym poziomem tej zdolności tj.: Wykonawca w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie - wykonał co najmniej jedną instalację logiczną na minimum 50 przyłączy komputerowych;

Ocena spełniania warunków wymienionych w ust. 3 dokonana zostanie zgodnie z formułą **„spełnia – nie spełnia”**, w oparciu o informacje zawarte w dokumentach i oświadczeniach wyszczególnionych w niniejszych Warunkach. Z treści załączonych dokumentów musi wynikać **jednoznacznie,** iż ww. warunki Wykonawca spełnił. **Niespełnienie chociażby jednego z warunków spowoduje wykluczenie Wykonawcy z postępowania o zamówienie. Ofertę Wykonawcy wykluczonego z postępowania uznaje się za odrzuconą.**

4. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia tj.: w formie konsorcjum lub spółki cywilnej, według następujących zasad:

4.1. **W odniesieniu do spółki cywilnej** upoważnią jednego spośród siebie, jako przedstawiciela pozostałych (wyznaczą pełnomocnika) do podpisania oferty, reprezentowania w postępowaniu albo do podpisania oferty, reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia, jeżeli z dokumentów dołączonych do oferty np. kopii umowy spółki poświadczonej odpowiednio za zgodność z oryginałem nie wynika odpowiedni sposób reprezentacji dla podpisania oferty. Pełnomocnictwo powinno być dołączone do oferty składanej w formie tradycyjnej (papierowe) i mieć formę oryginału lub poświadczonej notarialnie kopii oraz zawierać wyrażenie zgody na działanie zgodnie z niniejszymi Warunkami. Jeżeli oferta wraz z załącznikami zostanie złożona drogą elektroniczną (mailową) w formie skanu na adres marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, pełnomocnictwo o treści wyżej określonej, poświadczone notarialnie, powinno mieć również formę skanu. W przypadku złożenia oferty w formie elektronicznej, pełnomocnictwo o treści wyżej określonej, powinno być również złożone w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi.

4.2. **W odniesieniu do konsorcjum** - Wykonawcy upoważnią jednego spośród siebie, jako przedstawiciela pozostałych (wyznaczą pełnomocnika) do podpisania oferty, reprezentowania w postępowaniu o zamówienie albo do reprezentowania w postępowaniu o zamówienie i zawarcia umowy w tym postępowaniu. Wszelka korespondencja, zawarcie umowy oraz rozliczenia dokonywane **będą wyłącznie** z wyznaczonym pełnomocnikiem. Ustanowiony Pełnomocnik winien być upoważniony także do zaciągania zobowiązań i płatności w imieniu każdego partnera, na rzecz każdego z partnerów oraz do wyłącznego występowania w realizacji zawartej umowy o zamówienie. Pełnomocnictwo powinno być podpisane przez prawnie upoważnionych przedstawicieli każdego z partnerów i dołączone do oferty składanej w formie tradycyjnej, w postaci oryginału lub poświadczonej notarialnie kopii oraz zawierać wyrażenie zgody na działanie zgodnie z niniejszymi Warunkami. Jeżeli oferta wraz z załącznikami zostanie złożona drogą elektroniczną (mailową) w formie skanu na adres marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, pełnomocnictwo o treści wyżej określonej, poświadczone notarialnie, powinno mieć również formę skanu. W przypadku złożenia oferty w formie elektronicznej, pełnomocnictwo o treści wyżej określonej, powinno być również złożone w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi.

Uwaga: Treść pełnomocnictwa powinna dokładnie określać zakres umocowania.

5. Wykonawcy ubiegający się wspólnie o udzielenie zamówienia, dla potwierdzenia spełnienia warunków opisanych w części X ust. 3 pkt. 3.1, 3.2, 3.3 Warunków, składają wspólnie oświadczenia, o których mowa w części XI ust. 3 pkt 3.1, 3.2, 3.3.

6. Warunek udziału w postępowaniu o którym mowa w części X ust. 3 pkt. 3.4 musi spełnić co najmniej jeden z Wykonawców. Na potwierdzenie spełnienia tego warunku Wykonawcy składają oświadczenie o którym mowa w części XI ust. 4.

7. Wniesienie wadium musi wyraźnie wskazywać na wszystkich Wykonawców składających wspólną ofertę, chyba że Wykonawcy występujący wspólnie postanowią, iż wniesienia wadium dokona pełnomocnik konsorcjum – dotyczy konsorcjum. Zasady wnoszenia wadium opisane są szczegółowo w części XV.

8. Wykonawcy występujący wspólnie ponoszą solidarną odpowiedzialność wobec Zamawiającego za wykonanie Umowy i wniesienie zabezpieczenia należytego wykonania Umowy oraz za zobowiązania wynikające z gwarancji, gwarancji jakości, roszczeń z tytułu wad prawnych oprogramowań oraz rękojmi za wady prawne przedmiotu Umowy.

9. W przypadku wyboru oferty złożonej przez Wykonawców ubiegających się wspólnie o udzielenie zamówienia, na żądanie Zamawiającego, zobowiązani będą do przedłożenia, w tradycyjnej formie pisemnej, umowy regulującej współpracę Wykonawców – członków konsorcjum, a w odniesieniu do wspólników spółki cywilnej – w przypadku, jeżeli umowa spółki nie została dołączona do oferty. Po złożeniu oferty zmiany w składzie konsorcjum nie są dopuszczalne.

XI <u>Dokumenty składane przez Wykonawcę celem wykazania braku podstaw do wykluczenia, potwierdzenia spełnienia warunków określonych w niniejszym zapytaniu ofertowym oraz inne dokumenty określone w niniejszych Warunkach zapytania:</u>

1. W celu potwierdzenia niepodlegania wykluczeniu z postępowania Wykonawca zobowiązany jest przedłożyć następujące dokumenty, <u>aktualne na dzień składania ofert</u>:

   1) oświadczenie o braku powiązań kapitałowych i personalnych, o których mowa w **podrozdziale 6.5.2 „Zasada konkurencyjności" pkt 2 lit. a** Wytycznych zgodnie **z Załącznikiem nr 4** do niniejszych Warunków, przedkładanym wraz z ofertą. W odniesieniu do podmiotów posiadających organ zarządzający i/lub nadzorczy **<u>oświadczenie składa każdy członek wymienionych organów</u>**. Jeżeli Wykonawcą jest spółka cywilna lub handlowa spółka osobowa - oświadczenie składa każdy wspólnik. Jeżeli Wykonawca działa przez prokurenta (prokurentów) oświadczenie to składa każdy prokurent. Jeżeli Wykonawca działa przez pełnomocnika (pełnomocników) oświadczenie to składa każdy pełnomocnik;
   2) informację z Krajowego Rejestru Karnego w zakresie określonym w części X ust. 2 pkt. 2.2, 2.3 i pkt. 2.6 wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
   3) aktualny odpis z KRS - rejestru przedsiębiorców lub CEIDG w celu wykazania braku podstaw do wykluczenia o których mowa w części X ust 2. pkt 2.7,.

2 **W przypadku ubiegania się o udzielenie niniejszego zamówienia wspólnie przez dwóch lub więcej Wykonawców w ofercie muszę być złożone dokumenty wymienione w ust. 1 oddzielnie dla każdego Wykonawcy.**

3 Sposób i forma złożenia oświadczeń, o których mowa w ust 1 pkt 1) –pkt 3) oraz w ust. 2, obowiązuje w przypadku złożenia oferty w formie tradycyjnej (papierowej). Jeżeli oferta składana jest drogą elektroniczną (mailową) w formie skanu na adres: marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, oświadczenia o których mowa w ust 1 pkt 1) –pkt) 3 oraz w ust. 2 podpisane przez Wykonawcę/ów, przedkładane są również w formie skanu – zgodnie z wyżej określonymi zasadami. W przypadku składania oferty w formie elektronicznej, oświadczenia Wykonawcy/ów, o których mowa ust 1 pkt 1) –pkt) 3 oraz w ust. 2, powinny być również złożone w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi – zgodnie z wyżej określonymi zasadami.

4 W celu wykazania spełnienia warunków, o których mowa w części X ust. 3 pkt 3.1, 3.2, 3.3, Wykonawca oświadcza**, że na dzień składania oferty**:

1) posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2) znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie przedmiotu zamówienia we wskazanym terminie;
3) posiada niezbędną wiedzę i doświadczenie oraz dysponuje odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania zamówienia.

5. Oświadczenia Wykonawcy/ów, który/którzy składa/ją ofertę w formie tradycyjnej (papierowej) składane są na piśmie w oryginale zgodnie **z Załącznikiem nr 5** do niniejszych Warunków i przedkładane są wraz z ofertą. Jeżeli oferta składana jest drogą elektroniczną (mailową) w formie skanu na adres marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, oświadczenia podpisane przez Wykonawcę/ów, zgodnie **z Załącznikiem Nr 5**, przedkładane są również w formie skanu i składane wraz z ofertą. W przypadku składania oferty w formie elektronicznej, oświadczenia Wykonawcy/ów, złożone zgodnie z **Załącznikiem Nr 5**, powinny być również przedłożone w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi.

7. W celu wykazania spełnienia warunku, o którym mowa w części X ust. 3 pkt 3.4 Wykonawca przedkłada oświadczenie zgodnie z **Załącznikiem Nr 6**, dołączając dokumenty potwierdzające należyte wykonanie prac określonych w tym Załączniku. Jeżeli oferta składana jest drogą elektroniczną (mailową) w formie skanu na adres poczty elektronicznej marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, oświadczenie podpisane przez Wykonawcę/ów, zgodnie z **Załącznikiem Nr 6**, przedkładane są również w formie skanu i składane wraz z ofertą. W przypadku składania oferty w formie elektronicznej, oświadczenia Wykonawcy/ów, złożone zgodnie z **Załącznikiem Nr 6**, powinny być również złożone w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi.

8. **Inne wymagane dokumenty:**
   1) formularz ofertowy zgodnie **z Załącznikiem nr 3** do niniejszych Warunków;
   2) pełnomocnictwo;
   3) klauzula informacyjna Zamawiającego wraz z oświadczeniem Wykonawcy zgodnie **z Załącznikiem nr 7** do niniejszych Warunków,
   4) parafowany wzór dokumentu gwarancyjnego zgodnie **z Załącznikiem nr 8** do niniejszych Warunków,
   5) parafowany wzór Umowy zgodnie **z Załącznikiem nr 9** do niniejszych Warunków,

Oświadczenie, o którym mowa w pkt. 3 składa każda osoba fizyczna, której dane osobowe będą przetwarzane przez Zamawiającego w związku ze złożeniem Oferty - zgodnie **z Załącznikiem nr 7** do niniejszych Warunków.

Do oferty należy dołączyć pełnomocnictwo (pełnomocnictwa) w formie oryginału lub kopii poświadczonej za zgodność z oryginałem, jeżeli oferta będzie podpisana przez pełnomocnika, przy czym dotyczy to również przypadków Wykonawców składających ofertę wspólnie.

9. Wszystkie dokumenty i oświadczenia, o których mowa w ust. 7 powinny być złożone odpowiednio – w zależności od formy złożenia oferty – w formie papierowej lub skanu podpisanych dokumentów i oświadczeń – jeżeli w takiej formie składana jest oferta lub w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi – jeżeli w takiej formie składana jest oferta.
10. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania, poza terytorium Rzeczypospolitej Polskiej i nie może przedłożyć dokumentów wymienionych w części XI ust. 1 pkt. 2, pkt. 3 – składa ich odpowiedniki wystawione w terminach tam określonych, pozwalające na ocenę przesłanek braku wykluczenia i spełnienia warunków udziału w postępowaniu.
11. Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w części XI ust. 1 pkt. 2, pkt. 3, zastępuje się je dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju pochodzenia osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania.
12. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
13. **Jeżeli Wykonawca nie złożył wszystkich wymaganych przez Zamawiającego oświadczeń i dokumentów wymienionych w części XI niniejszych Warunków; oświadczenia lub dokumenty są: niekompletne, złożone w niewłaściwej formie, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia w terminie przez siebie wskazanym. Powyższe nie dotyczy treści formularza oferty, o którym mowa w ust. 7 pkt 1.**

14. W przypadku, gdy Wykonawca nie zastosuje się do wezwania, o którym mowa w ust. 12 Wykonawcę uznaję się za wykluczonego z postępowania, a oferta jego podlega odrzuceniu.

XII. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz wskazanie osób do porozumiewania się z Wykonawcami:

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Warunków w formie zapytania, za pośrednictwem:
   1) poczty elektronicznej na adres marek.rogalski@wspia.eu; w temacie wiadomości należy wpisać numer referencyjny zapytania ofertowego 8/KON/z045/2021; treść zapytania powinna być podpisana przez upoważnioną osobę/osoby i przesłana jako skan;
   2) za pośrednictwem strony https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, zgodnie z „Instrukcją Oferenta w BK2021"
2. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 5 dni przed upływem terminu składania ofert - pod warunkiem że wniosek wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
3. Jeżeli wniosek o wyjaśnienie treści Warunków wpłynął po upływie terminu składania wniosku, o którym mowa w ust. 2, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpatrywania.
4. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w ust. 2.
5. Treść zapytań wraz z wyjaśnieniami Zamawiający zamieszcza **wyłącznie** na stronie internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/. **Treść odpowiedzi na zapytania powinna być uwzględniona przez wszystkich Wykonawców w składanych przez nich ofertach.**
6. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść Warunków do niniejszego zapytania ofertowego. Dokonaną zmianę Warunków Zamawiający zamieszcza na stronie internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/.
7. Postępowanie w związku z niniejszym zapytaniem ofertowym prowadzi się w języku polskim.
8. W niniejszym postępowaniu zawiadomienia lub informacje (poza wyjaśnieniami o których mowa w ust. 1) Zamawiający i Wykonawcy przekazują, za potwierdzeniem odbioru i odczytu. drogą elektroniczną (e-mail).
9. Osobą upoważnioną do kontaktu z Wykonawcami jest:
   mgr Marek Rogalski;
   email: marek.rogalski@wspia.eu;
   telefon: 17 867 04 46.

XIII. Opis sposobu przygotowania oferty:

1. Ofertę wraz z załącznikami można złożyć w jednej z następujących form:
   1) w tradycyjnej formie pisemnej (papierowej);
   2) w formie skanu przesłanego na adres poczty elektronicznej marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, przy czym wszystkie dokumenty muszą być wcześniej podpisane przez upoważnioną/e osobę/osoby ze strony Wykonawcy, z uwzględnieniem zasad dotyczących udzielenia pełnomocnictwa, a następnie zeskanowane; w formie elektronicznej z podpisem/podpisami elektronicznymi lub opatrzone podpisem/podpisami zaufanym/zaufanymi złożonymi przez osobę/y upoważnione do reprezentowania Wykonawcy/ów, zgodnie z zasadami reprezentacji określonymi w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

2. Wykonawca może złożyć tylko jedną ofertę uwzględniającą odrębnie wycenę Systemu nr 1, Systemu nr 2, wraz z ich instalacjami i wdrożeniami zgodnie z treścią formularzu ofertowego stanowiącego **Załącznik nr 3** do niniejszych Warunków.
3. Zamawiający nie dopuszcza składania ofert częściowych, ani też ofert wariantowych.
4. Wykonawcy mogą wspólnie złożyć ofertę na zasadach określonych w niniejszych Warunkach. W takim przypadku na formularzu ofertowym, jak również innych dokumentach składanych przez Wykonawcę, w miejscu „*nazwa i adres Wykonawcy*" należy wpisać dane dotyczące konsorcjum lub spółki cywilnej ze wskazaniem pełnomocnika, który reprezentuje podmioty działające łącznie.
5. Wszelkie koszty związane ze sporządzeniem oraz złożeniem oferty ponosi Wykonawca niezależnie od wyniku postępowania.
6. **Systemy: Nr 1 i Nr 2 wraz z ich instalacjami i wdrożeniami muszą być zgodne z wymogami zawartymi odpowiednio w Specyfikacjach: Nr 1 i Nr 2. Na tę okoliczność Wykonawca dołącza do oferty Specyfikacje Nr 1 i Nr 2, których strony są parafowane przez uprawnione osoby (z uwzględnieniem zapisu ust. 7). W przypadku złożenia oferty przez Wykonawcę, w której wymagania w odniesieniu chociażby do jednego z Systemu przedmiotu zamówienia nie zostaną spełnione, oferta tego Wykonawcy/ów podlegać będzie odrzuceniu bez wezwania do jej uzupełnienia w tym zakresie. Zamawiający dopuszcza jedynie uzupełnienie wady formalnej Specyfikacji polegających na braku zaparafowania ich stron.**
7. W przypadku użycia w niniejszych Warunkach, w tym w Specyfikacjach Technicznych nazw własnych, Zamawiający dopuszcza rozwiązania równoważne.
8. Wykonawca, przy oferowaniu rozwiązań innych niż wzorcowe wskazanych w Specyfikacjach, musi szczegółowo wykazać w treści oferty ich równoważność z warunkami i wymaganiami opisanymi w Specyfikacjach. W tym celu, zobowiązany jest dołączyć do oferty ich szczegółowe opisy i dokumenty pozwalające Zamawiającemu na skuteczną ocenę zgodności oferowanych elementów przedmiotu zamówienia z wymaganiami Zamawiającego. Wykonawca poda w ofercie wykaz zastosowanych produktów (rozwiązań) równoważnych, z uwzględnieniem w szczególności: nazwy producenta, zakresu funkcjonalności oferowanego oprogramowania oraz opisu jego właściwości technicznych i/lub funkcjonalnych (katalogi, foldery, prospekty, itp.). Zastosowane technologie powinny spełniać wszystkie obowiązujące normy i być dopuszczone do obrotu na terenie Polski i Unii Europejskiej. Wskazane w Specyfikacji nazwy własne, symbole, modele, typy i itp. mają jedynie charakter wzorcowy. **W przypadku niewykazania przez Wykonawcę rozwiązań równoważnych w sposób wyżej wymieniony oferta Wykonawcy/ów podlega odrzuceniu bez wezwania do jej uzupełnienia. Zamawiający dopuszcza jedynie uzupełnienie wady formalnej Specyfikacji polegających na braku zaparafowania ich stron.**
9. Każda oferta powinna być napisana w języku polskim. **Podpisy złożone przez uprawnione osoby, o których mowa w ust 11, powinny umożliwiać jednoznaczną identyfikację tych osób**.
10. Należy ponumerować wszystkie strony oferty, a w przypadku gdy oferta zostanie złożona w formie, o której mowa w ust. 1 pkt 1), ponadto należy spiąć tę ofertę w sposób uniemożliwiający wysunięcie się którejkolwiek kartki.
11. Oferta i wymagane dokumenty wskazane w Warunkach muszą być podpisana przez osobę (osoby) uprawnione do składania oświadczeń woli w imieniu Wykonawcy, w tym zaciągania zobowiązań w wysokości odpowiadającej cenie oferty lub przez pełnomocnika/ów. W przypadku podpisania oferty przez pełnomocnika **stosować należy odpowiednio wszystkie reguły określone w części X ust. 4.**
12. Wszelkie poprawki lub zmiany w tekście oferty złożonej w formie, o której mowa w ust. 1 pkt 1 i pkt 2) muszą być parafowane własnoręcznie przez osobę/y podpisującą/e ofertę; w przeciwnym razie nie będą uwzględniane.

13. **Ofertę składaną w tradycyjnej formie pisemnej należy złożyć w dwóch zamkniętych kopertach (innych opakowaniach): zewnętrznej i wewnętrznej.**

    Na kopercie zewnętrznej należy napisać:

    WSPiA Rzeszowska Szkoła Wyższa
    ul. Cegielniana 14, 35-310 Rzeszów.
    OFERTA NA ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI
    w ramach projektu pn.:
    „NOWY WYMIAR STUDIOWANIA w WSPIA"
    WND POWR.03.05.00-00-z045/17, działanie 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego.
    NIE OTWIERAĆ PRZED dniem 1 czerwca 2021 r.

14. Wykonawca może wprowadzić zmiany, poprawki i uzupełnienia do złożonej oferty – w takiej samej formie jak złożona oferta - pod warunkiem, że Zamawiający otrzyma oświadczenie o wprowadzeniu zmian, poprawek lub uzupełnień przed terminem składania ofert. Oświadczenie o wprowadzeniu zmian, poprawek lub uzupełnień musi być złożone wg. takich samych zasad jak składanie ofert. Jeżeli oferta została złożona w tradycyjnej formie pisemnej - na kopercie należy zamieścić dopisek: **„ZMIANA"** lub **„UZUPEŁNIENIE"** Koperta oznakowana dopiskiem **„ZMIANA"** lub **„UZUPEŁNIENIE"** zostanie otwarta przy otwieraniu oferty Wykonawcy złożonej w tej formie. Jeżeli oferta została przesłana na adres poczty elektronicznej marek.rogalski@wspia.eu lub za pośrednictwem strony internetowej https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, Wykonawca w takiej samej formie informuje Zamawiającego o dokonanej zmianie lub uzupełnieniu oferty, oznaczając odpowiednio dokument, zamieszczając podpisy uprawnionych osób skanując go i przesyłając w analogiczny sposób jak ofertę. Skan pisma zawierającego zmiany lub uzupełnienie oferty zostanie dołączony do oferty. Jeżeli oferta jest złożona elektronicznie z podpisem/podpisami elektronicznymi lub opatrzona podpisem/podpisami zaufanym/zaufanymi – zmiana lub uzupełnienie oferty dokonywana jest w tej samej formie.

Oferta, jej zmiana lub uzupełnienie złożone po terminie wyznaczonym na składanie ofert, zostaną zwrócone Wykonawcy – bez otwierania.

15. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie powiadomienia w takiej samej formie i wg takich samych zasad jak wprowadzanie zmian, poprawek lub uzupełnień z oświadczeniem że oferta zostaje **„WYCOFANA".**

XIV Sposób zamieszczania w ofercie informacji o tajemnicy przedsiębiorstwa:

1. Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (j.t. Dz. U. z 2019 r. poz. 1010 z późn. zm.) rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności tzn. zastrzegł składając ofertę, iż nie mogą być one udostępnione innym Oferentom. Stosowne zastrzeżenie Wykonawca winien złożyć na formularzu ofertowym **(wg Załącznika nr 3 do Warunków)**. W przeciwnym razie treść całej oferty jest jawna.
2. **Zamawiający wskazuje, że informacje zastrzeżone jako tajemnica przedsiębiorstwa powinny być złożone przez Wykonawcę w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa" – jeżeli oferta zostaje złozona w tradycyjnej pisemnej formie - lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty w tej formie. W przypadku gdy oferta zostaje składana w innych formach określonych przez Zamawiającego w Cz. XIII ust. 1. pkt 2) i pkt 3) – zastrzeżenie tajemnicy jest składane w takiej samej formie.**
3. Wykonawca nie może zastrzec jako tajemnicy przedsiębiorstwa, elementów oferty, zawartych w jej treści i Załącznikach, które podlegają ocenie w niniejszym postępowaniu ofertowym i dowodzą spełnienia warunków udziału w postępowaniu oraz braku przesłanek wykluczenie z tego postępowania. Elementy te są jawne i po rozstrzygnięciu postępowania i mogą być udostępniane na wniosek zainteresowanych.

XV Wadium:

1. Każda oferta musi być zabezpieczona wadium o wartości 4 500 zł (słownie: cztery tysiące pięćset złotych 00/100).
2. Wadium może być wniesione w jednej z następujących form:
   1) w pieniądzu,
   2) w gwarancji bankowej;
   3) gwarancji ubezpieczeniowej;
3. **Wadium musi być wniesione przed wyznaczonym terminem składania ofert.** Wniesienie wadium w pieniądzu będzie skuteczne, jeżeli przed terminem składania ofert znajdzie się na rachunku bankowym Zamawiającego.
4. Wadium w formie pieniężnej należy wnieść na rachunek bankowy Zamawiającego prowadzony w Banku BGŻ BNP Paribas S.A., nr konta: 51 20300045 1110 0000 0090 6040 ze wskazaniem numeru zapytania ofertowego podanego w części II niniejszych Warunków.
5. Wadium wniesione w pieniądzu będzie przechowywane na nieoprocentowanym rachunku bankowym Zamawiającego nie dłużej niż okres związania ofertą określony w części II niniejszych Warunków.

6. Wadium wnoszone w formie: gwarancji bankowej lub gwarancji ubezpieczeniowej należy złożyć w oryginale u Zamawiającego – Wyższa Szkoła Prawa i Administracji Rzeszowska Szkoła Wyższa, 35-310 Rzeszów, ul Cegielniana 14. Wadium w oryginale powinno być złożone w kopercie z napisem „Wadium" ze wskazaniem numeru zapytania ofertowego podanego w części II niniejszych Warunków. Nie należy załączać oryginału dokumentu wadialnego do oferty jeżeli jest składana w tradycyjnej (pisemnej) formie. Wadium powinno obejmować okres wskazany w części XIX niniejszych Warunków.
7. Zamawiający zatrzymuje wadium w przypadku:
   1) uchylenie się Wykonawcy od zawarcia Umowy;
   2) niewniesienie zabezpieczenia należytego wykonania Umowy;
   3) zamieszczenia w ofercie nieprawdziwych oświadczeń lub informacji.

8. W przypadku wniesienia wadium w formie gwarancji bankowej lub ubezpieczeniowej konieczne jest, aby treść gwarancja obejmowała odpowiedzialność gwaranta za: uchylenie się Wykonawcy od zawarcia umowy, niewniesienie zabezpieczenia należytego wykonania umowy lub zamieszczenia w ofercie nieprawdziwych oświadczeń lub informacji. Z treści gwarancji musi jednoznacznie wynikać, jaki jest sposób reprezentacji gwaranta. Gwarancja musi być podpisana przez upoważnionego przedstawiciela gwaranta. Podpis winien być sporządzony w sposób umożliwiający jego identyfikację np. złożony wraz z imienną pieczątką lub czytelny - z podaniem imienia i nazwiska oraz stanowiska. Z treści gwarancji powinno wynikać bezwarunkowe, nieodwołalne, na każde pisemne żądanie zgłoszone przez Zamawiającego w terminie ważności gwarancji, zobowiązanie gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium oraz, że jest ona nieprzenoszalna.
9. Wykonawca, który nie wniesie wadium przed wyznaczonym terminem składania ofert lub wniesie go w innej formie niż określona w ust. 2 bądź wadium wniesione w innej formie niż pieniądzu nie będzie spełniać wymogów wskazanych w ust. 8 - nie zostanie objęty procedurą niniejszego postępowania ofertowego, w związku z czym oferta tego Wykonawcy bez otwierania zostanie zwrócona.
10. Zamawiający zwraca wadium Wykonawcom niezwłocznie po:
    1) wycofaniu oferty;
    2) wyborze najkorzystniejszej oferty z uwzględnieniem ust. 11;
    3) odrzuceniu oferty Wykonawcy w związku z niespełnieniem przesłanek materialnych i formalnych określonych w Warunkach;
    4) zamknięcia postępowania ofertowego bez wyboru którejkolwiek oferty.

11. Wadium Wykonawcy, którego oferta została wybrana będzie zwrócone po podpisaniu Umowy i wniesieniu zabezpieczenia jej wykonania. Wadium tego Wykonawcy zostanie zatrzymane albo dochodzone będzie z gwarancji w przypadku, gdy Wykonawca odmówi podpisania Umowy na warunkach określonych w ofercie, w tym także w przypadku niewniesienia wymaganego zabezpieczenia jej wykonania, a także w sytuacji gdy oświadczenia lub informacje zawarte w ofercie okażą się nieprawdziwe.

XVI Miejsce oraz termin składania ofert:

1. Ofertę w tradycyjnej pisemnej formie należy złożyć w WSPiA Rzeszowskiej Szkole Wyższej w Rzeszowie, ul. Cegielniana 14, 35-310 Rzeszów, budynek „A„ I piętro, pokój nr 1.02 - **do dnia 1 czerwca 2021 roku.** Oferty w innych formach dopuszczonych przez Zamawiającego należy złożyć **- do dnia 1 czerwca 2021 roku.**
2. Ofertę złożoną po terminie Zamawiający zwróci niezwłocznie Wykonawcy.

XVII Opis sposobu obliczenia ceny oferty:

1. Cenę oferty stanowić będzie **łączna wartość brutto** z podziałem tej kwoty na realizację Systemów: Nr 1 i Nr 2 wraz z ich instalacjami i wdrożeniami.
2. Podana w ofercie cena musi uwzględniać wszystkie wymagania Zamawiającego określone w niniejszych Warunkach oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami i warunkami realizacji przedmiotu zapytania ofertowego.
3. Podatek VAT należy naliczyć zgodnie z przepisami ustawy obowiązującymi na dzień składania oferty.
4. Jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania obowiązku podatkowego Zamawiającego zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami. Obowiązek podatkowy w sytuacji nabywania towarów lub usług od podmiotów zagranicznych, zgodnie z przepisami ustawy o podatku od towarów i usług, spoczywa na nabywcy towarów lub usługobiorcy, którym w przypadku postępowania o zamówienie jest Zamawiający. Dokonując wyboru – jako najkorzystniejszej – oferty Wykonawcy zagranicznego, z tytułu realizacji zobowiązania wynikającego z umowy, na podstawie obowiązujących przepisów podatkowych, na Zamawiającego zostaje nałożony obowiązek uiszczenia należnego podatku VAT. Podatek ten mimo, iż nie wchodzi w cenę oferty, tworzy wraz z nią rzeczywistą kwotę wydatkowanych środków publicznych. Z podobną sytuacją mamy do czynienia w przypadku dostawy towarów z państw trzecich. Tym samym dokonując czynności oceny ofert w zakresie kryterium ceny, Zamawiający jest zobowiązany dla porównania tych ofert doliczyć do ceny ofertowej podmiotów zagranicznych, kwoty należnego podatku VAT, który obciąża Zamawiającego z tytułu realizacji umowy. Zamawiający doliczy do ceny oferty również cło.
5. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w walucie polskiej (złoty polski). Zamawiający nie przewiduje rozliczenia w walutach obcych.
6. Łączną cenę oferty oraz poszczególnych jej elementów należy określać z dokładnością do dwóch miejsc po przecinku, stosownie do obowiązujących przepisów prawa.
7. Podmiot zagraniczny w formularzu cenowym wpisuje tylko cenę netto.
8. Zamawiający nie przewiduje udzielania zaliczek na poczet wykonania zamówienia.

XVIII Opis kryterium wyboru oferty wraz z podaniem jego wagi sposób oceny ofert:

1. Zamawiający oceniał będzie oferty według kryterium: **Łączna cena oferty brutto**. Waga 100%:
2. Cena oferty brutto (C) – Waga: 100% zostanie obliczone według formuły:

$$C = \frac{\text{najniższa oferowana cena brutto spośród badanych ofert}}{\text{cena oferty badanej brutto}} \times 100 \text{ pkt}$$

3. Oferta w kryterium cena może uzyskać maksymalnie 100 punktów. Końcowy wynik powyższego działania zostanie zaokrąglony do 2 miejsc po przecinku.

XIX Termin związania ofertą:

1. Wykonawca pozostaje związany ofertą przez okres 60 dni.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

XX Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia:

1. Zamawiający dokona wyboru oferty tego Wykonawcy, którego oferta odpowiada wszystkim wymogom określonym w niniejszych Warunkach i została oceniona jako najkorzystniejsza w oparciu o określone w Warunkach kryterium oceny.
2. Zamawiający niezwłocznie po wyborze najkorzystniejszej oferty powiadomi na piśmie pocztą elektroniczną wszystkich Wykonawców którzy złożyli oferty o:
   1) wyborze najkorzystniejszej oferty, podając nazwę (firmę), siedzibę i adres Wykonawcy, którego ofertę wybrano i uzasadnienie jej wyboru,
   2) Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne.
3. Zamawiający przed zawarciem Umowy wymaga przedłożenia:
   1) w tradycyjnej formie pisemnej umowy regulującej współpracę Wykonawców składających wspólnie ofertę w niniejszym postępowaniu w przypadku wyboru oferty tych Wykonawców;
   2) w tradycyjnej formie pisemnej Uchwały walnego zgromadzenia wspólników wyrażającej zgodę na zawarcie umowy - zgodnie z art. 230 kodeksu spółek handlowych, rozporządzenie prawem lub zaciągnięcie zobowiązania do świadczenia o wartości dwukrotnie przewyższającej wysokość kapitału zakładowego wymaga uchwały wspólników, chyba że umowa stanowi inaczej;
   3) do wglądu – oryginału oferty wraz z załącznikami – jeżeli oferta została złożona w formie skanu wszystkich wymaganych dokumentów w niniejszych Warunkach.
4. **Jeżeli Zamawiający stwierdzi, że skany przesłanych dokumentów są niezgodne z przedłożonymi oryginałami, unieważni niniejsze postępowanie o zamówienie i zatrzyma wadium.**
5. Zamawiający zawrze Umowę w sprawie dotyczącą realizację przedmiotu niniejszego zamówienia, w formie pisemnej, w terminie do 15 dni licząc od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.
6. O miejscu i terminie podpisania Umowy Zamawiający powiadomi wybranego Wykonawcę za pośrednictwem poczty elektronicznej.

7. Wykonawca zobowiązany jest **w terminie do 3 dni roboczych, licząc od daty zawarcia Umowy** złożyć lub wnieść zabezpieczenie należytego wykonania umowy, zgodnie z wymogami określonymi w części XXI Warunków.
8. W przypadku odmowy podpisania Umowy przez wybranego Wykonawcę, Zamawiający może zawrzeć Umowę z Wykonawcą, który spełnia wymagania zapytania ofertowego i którego oferta uzyskała kolejno najwyższą liczbę punktów.
9. Zamawiający dopuszcza możliwość prowadzenia negocjacji z Wykonawcą/Wykonawcami, którego/których oferta/oferty nie podlega/podlegają odrzuceniu, na etapie wyboru najkorzystniejszej oferty, a więc przed podpisaniem Umowy z Wykonawcą.

XXI Wymagania dotyczące zabezpieczenia należytego wykonania Umowy:

1. Zamawiający będzie żądać od Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, wniesienia zabezpieczenia należytego wykonania Umowy w wysokości 10 % ceny ofertowej (brutto).
2. Zabezpieczenie należytego wykonania Umowy gwarantuje zgodne z Umową wykonanie przedmiotu Umowy oraz służy do pokrycia roszczeń z tytułu gwarancji, rękojmi oraz roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, zapłaty kar umownych i odszkodowania uzupełniającego.
3. Zabezpieczenie należytego wykonania Umowy może być wniesione w następujących formach:
   1) gwarancji bankowej;
   2) gwarancji ubezpieczeniowej;
4. Gwarancja bankowa lub ubezpieczeniowa powinna być złożona w oryginale, musi być podpisana przez upoważnionego przedstawiciela gwaranta. Podpis winien być sporządzony w sposób umożliwiający jego identyfikację np. złożony wraz z imienną pieczątką lub czytelny (z podaniem imienia i nazwiska oraz stanowiska).
5. Gwarancja bankowa lub ubezpieczeniowa zabezpieczająca należyte wykonanie Umowy powinna zawierać stwierdzenia, iż bezwarunkowo, nieodwołalnie i na pierwsze pisemne wezwanie Zamawiającego do zapłacenia kwot tytułem nienależytego wykonania Umowy lub braku realizacji roszczeń Zamawiającego z tytułu gwarancji, rękojmi, zapłaty kar umownych i odszkodowania uzupełniającego następuje wypłata żądanej przez Zamawiającego kwoty bez jakichkolwiek zastrzeżeń ze strony gwaranta. W treści gwarancji powinno się znajdować też stwierdzenie, że gwarancja jest nieprzenoszalna.
6. 70% wniesionego zabezpieczenia należytego wykonania Umowy przeznacza się na zgodne z Umową wykonanie jej przedmiotu, a 30% wniesionego zabezpieczenia należytego wykonania Umowy jest przeznaczone na zabezpieczenie roszczeń z tytułu gwarancji, rękojmi, zapłaty kar umownych i odszkodowania uzupełniającego.
7. Pozostała część zabezpieczenia tj. 30% zostanie zwrócona Wykonawcy, w ciągu 30 dni po upływie okresu gwarancji i rękojmi.
8. Podane wyżej terminy na zwrot zabezpieczenia należytego wykonania Umowy rozpoczynają odpowiednio swój bieg - po protokolarnym bezusterkowym odbiorze przedmiotu Umowy oraz po protokolarnym stwierdzeniu usunięcia wszystkich wad, które ujawniły się w okresie gwarancji i rękojmi.

9. W przypadku przedłużenia terminu realizacji przedmiotu Umowy, Wykonawca przed podpisaniem stosownego aneksu w tym zakresie zobowiązany jest do przedłużenia terminu ważności wniesionego zabezpieczenia należytego wykonania Umowy lub do wniesienia nowego zabezpieczenia na okres realizacji Umowy wynikający z zawartego aneksu.
10. Wykonawca udzieli Zamawiającemu gwarancji na wykonany przedmiot Umowy zgodnie **z Załącznikiem nr 8** do niniejszych Warunków określającym wzór dokumentu gwarancyjnego.
11. Termin gwarancji wynosić będzie **36 miesięcy** i liczy się od dnia dokonania bezusterkowego odbioru końcowego przedmiotu Umowy. Dokument gwarancyjny Wykonawca zobowiązany jest dostarczyć w dniu odbioru końcowego jako załącznik do bezusterkowego protokołu odbioru końcowego przedmiotu Umowy.
12. W przypadku ujawnienia wad przedmiotu Umowy w okresie gwarancji, Zamawiający poinformuje o tym Wykonawcę na piśmie, określając termin ich usunięcia zgodnie z zawartą Umową i dokumentem gwarancyjnym.
13. W przypadku nieusunięcia wad w wskazanym przez Zamawiającego terminie, Zamawiający może naliczyć karę umowną zgodnie z postanowieniami Umowy oraz domagać się ich usunięcia od Wykonawcy względnie może powierzyć usunięcie wad osobie trzeciej, a powstałymi z tego tytułu kosztami obciążyć Wykonawcę, zachowując przy tym inne uprawnienia przysługujące mu na podstawie Umowy.
14. Niezależnie od udzielonej przez Wykonawcę gwarancji, Zamawiającemu przysługiwać będą roszczenia z tytułu rękojmi za wady, do których stosuje się przepisy Kodeksu cywilnego o rękojmi za wady oraz zawartą Umowę.
15. Wykonawca jest zobowiązany realizować roszczenia z tytułu rękojmi ponosząc wszelkie koszty z tym związane.

XXII Inne istotne dla Stron postanowienia, które zostaną wprowadzone do treści zawieranej Umowy w sprawie realizacji przedmiotu zamówienia:

1. **Umowa zostanie zawarta zgodnie z przedłożonym jej wzorem, stanowiącym Załącznik nr 9 do niniejszych Warunków. Wykonawca składający ofertę zobowiązany jest zapoznać się z wzorem Umowy oraz zaparafować każdą jej stronę.**
2. Zmiana warunków Umowy zawartej w wyniku przeprowadzonego postępowania o zamówienia może nastąpić jeżeli zachodzi **jedna z następujących okoliczności:**

2.1. zmiany umowy, niezależnie od ich wartości, nie są istotne z zastrzeżeniami wynikającym z Umowy.

Zmianę postanowień zawartej Umowy **uznaje się za istotną** jeżeli:

1) zmienia ona ogólny charakter umowy w stosunku do charakteru w pierwotnym brzmieniu;
2) nie zmienia ogólnego charakteru Umowy i zachodzi co najmniej jedna z następujących okoliczności:
   a) zmiana wprowadza warunki, które, gdyby były postawione w postępowaniu prowadzonym w związku z niniejszym zapytaniem, to w tym postępowaniu wzięliby lub mogliby wziąć udział inni wykonawcy lub przyjęto by oferty innej treści;
   b) zmiana narusza równowagę ekonomiczną Umowy na korzyść Wykonawcy w sposób nieprzewidziany pierwotnie w Umowie;
   c) zmiana znacznie rozszerza lub zmniejsza zakres świadczeń i zobowiązań wynikający z Umowy;

d) polega na zastąpieniu Wykonawcy, któremu Zamawiający udzielił zamówienia, nowym Wykonawcą, w innych przypadkach niż wymienione w pkt 2),

2.2. Wykonawcę, z którym Zamawiający zawarł Umowę w wyniku niniejszego postępowania ma zastąpić inny Wykonawca w wyniku połączenia, podziału, przekształcenia, upadłości, restrukturyzacji lub nabycia dotychczasowego Wykonawcy lub jego przedsiębiorstwa, o ile nowy Wykonawca spełnia warunki udziału w postępowaniu, nie zachodzą wobec niego przesłanki wykluczenia oraz nie powoduje to zmiany innych istotnych postanowień Umowy;

2.3. zostały spełnione łącznie następujące warunki, jeżeli nie prowadzą do zmiany charakteru Umowy:

a. konieczność zmiany spowodowana została okolicznościami, których Zamawiający, pomimo zachowania należytej staranności nie mógł przewidzieć;
b. wartość zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w Umowie.

3. Nie jest istotną zmianą Umowy przedłużenie terminu realizacji przedmiotu zamówienia o okres nie dłuższy niż 30 dni.
4. Możliwość przesunięcia terminu realizacji Umowy powyżej 30 dni uzależniona jest od uprzedniej zgody organu NCBR oraz od zaistnienia i udokumentowania okoliczności przemawiających za zmianą terminu, z korzyścią dla realizacji przedmiotu Umowy, na rzecz Zamawiającego.

XXIII <u>Pozostałe warunki zamówienia:</u>

1. Zamawiający może unieważnić niniejsze postępowanie w sprawie Zapytania ofertowego jeżeli:

   1) Zamawiający nie otrzymał dofinansowania ze środków publicznych na realizację przedmiotu zamówienia.
   2) Podmiot/podmioty biorące udział w postępowaniu wpłynęły na jego wynik w sposób sprzeczny z prawem lub Wytycznymi i zachodzi konieczność powtórzenia czynności prowadzonych w ramach postępowania o zamówienie;
   3) oferta z łączną najniższą ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia lub jeżeli cena na realizację chociażby jednego z Systemów (Systemu nr 1 wraz z wdrożeniem lub Systemu nr 2 wraz z wdrożeniem) w ofercie z najniższą łączną ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowania realizacji poszczególnych Systemów;
   4) wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć;
   5) zaistniała okoliczność, o której mowa w Cz. XX ust. 4 Warunków.
2. Zamawiający może zakończyć postępowanie bez wyboru którejkolwiek z ofert na każdym etapie postępowania podając przyczynę podjętej decyzji.

Załączniki:

1) Specyfikacja Techniczna nr 1,
2) Specyfikacja Techniczna nr 2,
3) Formularz ofertowy,
4) Oświadczenie Wykonawcy o braku powiązań osobowych i kapitałowych z Zamawiającym,
5) Oświadczenia złożone w celu wykazania spełnienia warunków o których mowa w części X ust. 3 pkt. 3.1., pkt. 3.2., pkt 3.3. Warunków,

6) Oświadczenia złożone w celu wykazania spełnienia warunków o których mowa w części X ust. 3 pkt 3.4. Warunków,
7) Klauzula informacyjna Zamawiającego,
8) Wzór dokumentu gwarancyjnego
9) Wzór umowy.

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 1 do Warunków

Specyfikacja Techniczna dotycząca System nr 1 - wyposażenia sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej wraz z ich instalacją i wdrożeniem. Celem umożliwienia studentom WSPiA zdawania egzaminów w systemie SBS, niezbędne jest wyposażenie posiadanej przez Uczelnię sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej obejmującej 232 stanowiska komputerowe.

I. Wykonanie przyłącza wraz z infrastrukturą – minimalne parametry:

1. STANDARDY ORAZ NORMY REFERENCYJNE

Podstawą do opracowania zagadnień związanych z koncepcją i instalacją okablowania strukturalnego są normy międzynarodowe i europejskie, które dla potrzeb tego projektu są referencyjne. Poniżej wymieniono obowiązujące standardy na których oparto niniejszy projekt:

Normy dotyczące okablowania strukturalnego:
- *ISO/IEC 11801:2010 (Ed. 2.2) Information technology — Generic cabling for customer premises*
- *EN 50173-1:2011 Information Technology – Generic cabling systems – Part.1 Generic requirements*

lub z polską edycją normy:
- *PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne*
- *EN 50173-1:2011* Information Technology - Generic cabling systems – Part.2 Office premises

lub z polską edycją normy:
- *PN-EN 50173-2:2008 Technika Informatyczna – Systemy okablowania strukturalnego – Część 2: Budynki biurowe;*

Normy referencyjne dotyczące instalacji i pomiarów:
- *EN 50174-1:2010 Information Technology - Cabling system installation- Part 1. Specification and quality assurance*

lub z polską edycją normy:
- *PN-EN 50174-1:2010 Technika informatyczna. Instalacja okablowania – Część 1- Specyfikacja i zapewnienie jakości;*
- *EN 50174-2:2010 Information Technology - Cabling system installation - Part 2. Installation planning and practices internal to buildings*

lub z polską edycją normy:
- *PN-EN 50174-2:2010 Technika informatyczna. Instalacja okablowania – Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;*
- *EN 50346:2004 Information Technology - Cabling system installation - Testing of installed cabling*

lub z polską edycją normy:
- *PN-EN 50346:2004 Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania*
- *EN 50310:2012 Application of equipotential bonding and earthling at premises with information technology equipment.*

lub z polską edycją normy:
- *PN-EN 50310:2012 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym;*
- *EN 61935-1:2009 Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards*

lub z polską edycją normy:

- *PN-EN 61935-1:2010E Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii telekomunikacyjnych -- Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm EN 50173*
- *ISO/IEC 14763-3:2006/A1:2009 Information technology –Implementation and operation of customer premises cabling – Part 3: Testing of optical fiber cabling*

lub z polską edycją normy:

- *PN-ISO/IEC 14763-3:2009/A1:2010P Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego*

2. ZAŁOŻENIA PODSTAWOWE – WYTYCZNE UŻYTKOWNIKA

- Lokalizacja, ilość i wielkość stanowisk roboczych wynika z wskazówek Użytkownika końcowego;
- Wszystkie elementy pasywne składające się na okablowanie strukturalne muszą być oznaczone nazwą lub znakiem firmowym, tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego w/w producenta;
- Producent okablowania strukturalnego musi legitymować się ważnym certyfikatem systemu zarządzania ISO9001:2008 od minimum 10 lat co gwarantuje Użytkownikowi właściwą obsługę procesów sprzedażowych i utrzymaniowych.
- System okablowania strukturalnego zaprojektowano w wersji ekranowanej ma posiadać wydajność klasy E zgodnie z normami referencyjnymi potwierdzoną przez uznane, niezależne laboratorium (np. 3P, GHMT)
- Środowisko, w którym będzie instalowany osprzęt kablowy jest środowiskiem biurowym i zostało ono sklasyfikowane, jako łagodne wg. skali $M_1I_1C_1E_1$ zgodnie z EN 50173-1:2011;
- Podsystem okablowania poziomego w zakresie łączy miedzianych zrealizowany zostanie w oparciu o ekranowany kabel Kategorii 6 w wersji ekranowania: U/FTP. W celu zagwarantowania niezbędnych marginesów pracy ze względu na długi okres użytkowania sieci kabel musi być przebadany w pasmie do 400 MHz. Osłona zewnętrzna musi być typu LSZH. Ze względu na gabaryty duktów przyjętych w projekcie dopuszcza się kable o średnicach zewnętrznych max. 6,9mm. W celach identyfikacyjnych wymaga się aby powłoka zewnętrzna kabla była w kolorze turkusowym. Na drogach ewakuacyjnych należy zastosować kabel zgodnie z CPR(EN 50575) Dca-s2,d1,a1.
- Podsystem okablowania poziomego w części światłowodowej oparty zostanie na okablowaniu wielomodowym (zwanym dalej MM). Okablowanie MM charakteryzować się będzie kategorią włókien OM3 według ISO/IEC 11801 Ed.2.2: 2011. Interfejsem światłowodowym dedykowanym w całej sieci jest LC/PC.
- Konfiguracja oraz rozmieszczenie gniazd końcowych przedstawiona została na podkładach i schematach dołączonych do projektu;
- Okablowanie ma być zrealizowane w oparciu o ekranowany moduł gniazda RJ45 Kat. 6 FTP
- Zgodnie z wymaganiami norm każdy 4 – parowy kabel ma być trwale zakończony na ekranowanym module RJ45 umieszczonym w gnieździe od strony użytkownika oraz na panelu krosowym w szafie;
- Panele krosowe 48 portowe w Głównych Punktach Dystrybucyjnych mają mieć wysokość 1U charakteryzować się budową modularną tak aby można było zastosować ten sam standard mocowania modułów przyłączeniowych po obu stronach toru. Panele muszą być wyposażone w półkę kablową oraz posiadać dedykowane miejsce na przypięcie uziemienia.
- Poszczególne punkty dystrybucyjne zostały zaprojektowane zgodnie z ISO/IEC 11801 Ed.2.2: 2011. Dystrybutor Budynkowy określono jako GPD.
  - GPD oparto na szafach dystrybucyjnych 19”, 33U o wymiarach 600x600mm
- W GPD przewidziano osprzęt do zakończenia kabli światłowodowych stanowiących połączenia poziome.
- Punkt abonencki PEL oparty zostanie na płycie czołowej adapterze dopasowanym do standardu gniazd elektrycznych wybranych przez inwestora z możliwością montażu dwóch modułów gniazd RJ45/s. Gniazdo powinno mieć możliwość zaimplementowania kodowania kolorem w dowolnym momencie eksploatacji, tożsamym z systemem kodowania kolorem zaimplementowanych na kablach przyłączeniowych
- W celu zagwarantowania jak najwyższych marginesów pracy i zapasów parametrów transmisyjnych nie dopuszcza się rozwiązań złożonych z elementów różnych producentów, (tj. kabla, gniazd, kabli krosowych, itp.). Aby zagwarantować rzeczywiste i powtarzalne parametry toru oraz potwierdzić zgodność

proponowanego rozwiązania z najnowszymi edycjami obowiązujących standardów międzynarodowych i niezależność od dostawcy komponentów wymagane jest na etapie oferty przedstawienie odpowiednich certyfikatów wydanych przez niezależne laboratoria uwzględniające najnowszą metodę kwalifikacji komponentów sieciowych.

3. ZAŁOŻENIA SZCZEGÓŁOWE PROJEKTOWE

3.1 PODSYSTEM OKABLOWANIA POZIOMEGO

Zgodnie z normami referencyjnymi podsystem okablowania poziomego może realizować zarówno połączenia miedziane jak i światłowodowe pomiędzy punktami PEL a GPD. Dla potrzeb tego projektu przyjęto założenie, że podsystem okablowania poziomego składa się z okablowania miedzianego o wydajności klasy E oraz okablowania światłowodowego SM kategorii OS2/G.652.D.

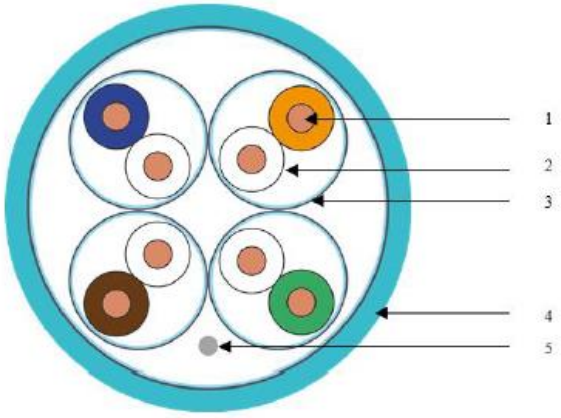
3.1.1 PODSYSTEM OKABLOWANIA POZIOMEGO –POŁĄCZENIA MIEDZIANE

3.1.1.1 Miedziany kabel instalacyjny

Miedziany kabel instalacyjny musi cechować się szeregiem własności zarówno transmisyjnych jak i mechanicznych. Wymagane właściwości kabla przedstawia tabela poniżej:

Kategoria zgodnie z ISO11801 ed.2.2.	6
Klasyfikacja ogniowa	IEC 60332-1; IEC 60754-2; IEC 61034, Dca-s2,d1,a1
Ekranowanie	U/FTP
Klasa separacji	C
Zakres częstotliwości [MHz]	400
ø żył [AWG]	23
Max ø zewnętrzna kabla mm]	6,9
Min promień gięcia instalacja [mm]	8xD
Min promień gięcia użytkowanie [mm]	4xD
Max Waga [kg/km]	47,5
NVP	79

Tabela 1. Wymagane właściwości dla kabla miedzianego segmentu okablowania poziomego



KONSTRUKCJA:

1 – Przewodnik
Materiał: drut miedziany.
Średnica nominalna: 23 AWG
2 – Izolacja
Materiał: miękki polietylen.
Średnica nominalna: 1.4 mm.
Skręcone przewody
Para: 2 skręcone żyły izolowane.
Ilość par: 4, wszystkie skręcone razem.
3 – Indywidualny ekran: aluminium / taśma poliestrowa.
4 – Płaszcz
Materiał: LSZH
Kolor: niebieski (RAL 5015)
5 – Drut drenu cynowany drut miedziany

Rysunek 1. Przekrój poprzeczny przykładowego kabla instalacyjnego kat 6 U/FTP Dca-s2,d1,a1.

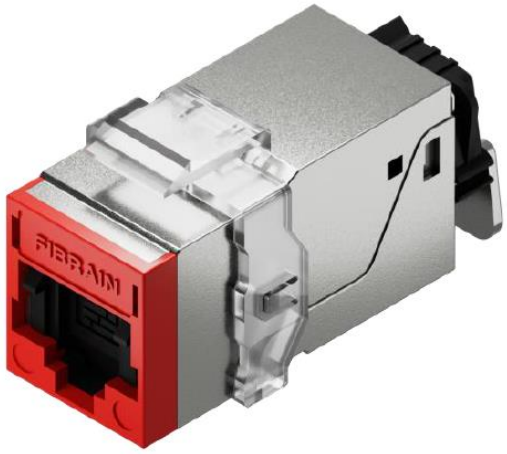
3.1.1.2 Moduły przyłączeniowe

Moduły przyłączeniowe stanowią kluczowy element zapewniający poprawna transmisje danych. Moduł przyłączeniowy musi charakteryzować się następującymi własnościami:
- Moduł musi charakteryzować się wydajnością Kat.6 zgodnie ze standardami ISO 11801-x:2017, EN-50173-x:2018. Powyższe musi zostać potwierdzone stosownym certyfikatem na komponent wystawionym przez uznane niezależne laboratorium badawcze np. Delta, GHMT, 3P.
- Wymaga się aby ze względów ułatwiających logistykę stosowano ten sam rodzaj modułu zarówno po stronie panela jak i PEL.
- Sposób mocowania modułu przyłączeniowego w miejscu instalacji powinien być elastyczny umożliwiając instalację również w oprawach/gniazdach wyprodukowanych przez firmy 3cie. Powyższe powinno się realizować za pomocą odpowiedniego adaptera (np. keystone) zatrzaskiwanego na korpusie modułu.
- Sposób terminacji żył kabla w module musi być wykonany za pomocą technologii IDC, jako powszechnie uznaną za najbardziej niezawodną metodę terminacyjną.
- Żyły kabla zarabianego na module muszą być blokowane w samym module tak aby zabezpieczyć miejsce styku na nożach IDC przed poluzowaniem się np. wskutek wibracji
- Moduł musi posiadać uchylną osłonę przeciwkurzową w różnych kolorach tak aby uzyskać również funkcjonalność kodowania kolorem za pomocą jednego elementu.
- Metoda terminacji kabla instalacyjnego na module musi gwarantować niezależność jakości uzyskanego kontaktu od stanu i jakości narzędzi niezbędnych do zarabiania łączy. W związku z powyższym moduł powinien umożliwiać zarabianie go na kablu instalacyjnym beznarzędziowo czyli bez konieczności stosowania dedykowanych do tego celu urządzeń.
- Moduł musi zapewniać trwałość połączenia kabel-moduł poprzez przytwierdzenie kabla instalacyjnego do obudowy modułu. Ze względu na ewentualne reterminacje element przytwierdzający kabel do modułu musi charakteryzować się możliwością wielokrotnego użycia bez konieczności każdorazowej jego wymiany.
- Ekranowanie modułu musi zapewniać ochronę 360˚
- Styk ekranowania kabla instalacyjnego z ekranem modułu musi gwarantować przejście o minimalnej impedancji, czyli powierzchnia samego styku powinna być odpowiednio duża
- Z uwagi na konieczność zapewnienia zdalnego zasilania urządzeń peryferyjnych podpiętych do sieci, użyte moduły przyłączeniowe muszą wspierać standardy IEEE 802.3af/802.3at (PoE/PoE+).

Pozostałe wymagane właściwości modułu przedstawia tabela poniżej:

Kategoria zgodnie z ISO11801 ed.2.2.	6
Zakres ø żył kabla [AWG]	26-22
Min ilość cykli połączeniowych	750
Schematy rozszycia kabla	TIA 568A/B
Trwałość IDC	>750 cykli łączeniowych
Niepalność obudowy	UL94V-0

Tabela 2. Wymagane właściwości dla modułu przyłączeniowego



Rysunek 2. Moduł przyłączeniowy kat 6 FTP

3.1.1.3 Miedziane kable przyłączeniowe

Miedziane kable przyłączeniowe stanowią połączenie aktywnych urządzeń sieciowych z infrastruktura pasywną sieci. Projekt zakłada zastosowanie kabli przyłączeniowych o takich samych parametrach wydajnościowych (kategorii) co inne elementy okablowania strukturalnego (kable instalacyjne, moduły przyłączeniowe).
- Kable przyłączeniowe muszą prezentować marginesy pracy dla zapewnienia poprawności obsługi wszystkich aplikacji transmisji danych również tych, które zostaną opracowane w przyszłości.
- Kable krosowe, w dowolnym momencie eksploatacji muszą posiadać możliwość doposażenia ich w elementy umożliwiające kodowanie kolorem co ułatwia administrowanie infrastruktura pasywna w czasie eksploatacji
- Kable przyłączeniowe muszą być wyposażone w tzw. boot czyli element zapewniający właściwe promienie gięcia kabla przyłączeniowego
- Kable przyłączeniowe muszą być wyposażone w element zabezpieczający przed wyłamaniem języczka/spustu będącego elementem konstrukcyjnym wtyku RJ45.
- posiadać system separacji par wewnątrz wtyku RJ45 w postaci separatora krzyżakowego, w celu redukcji przesłuchów między poszczególnymi parami.

Pozostałe wymagane właściwości kabli przyłączeniowych przedstawia tabela poniżej:

Kategoria zgodnie z ISO11801 ed.2.2.	6_A
Klasyfikacja ogniowa	LSFRZH - IEC 60332-3-24; IEC 60754-2; IEC 61034
Ekranowanie	S/FTP

Tabela 3. Wymagane właściwości dla kabli przyłączeniowych

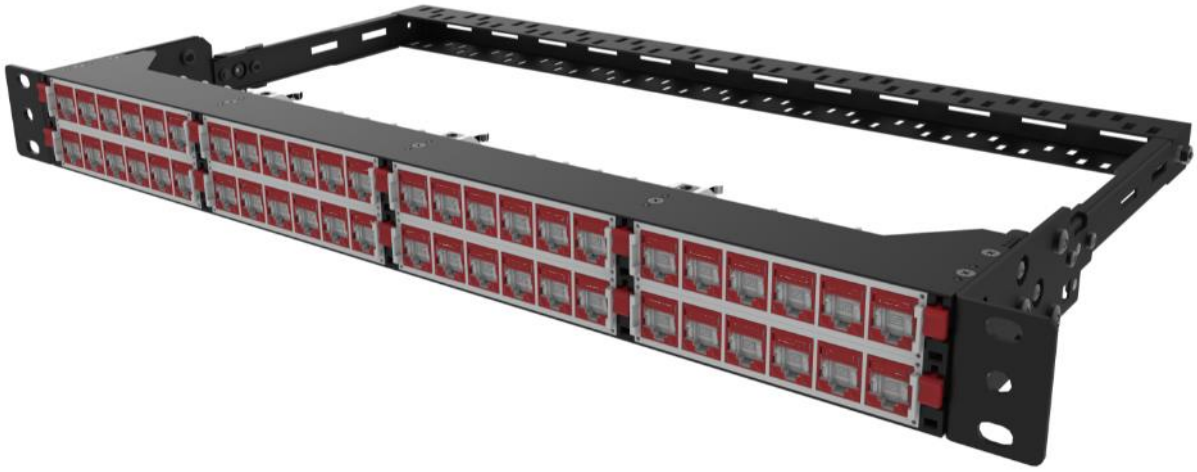
Rysunek 3. Schemat elementów składowych miedzianych kabli przyłączeniowych kat. 6a S/FTP

3.1.1.4 Panele krosowe

Wyspecyfikowane powyżej kable miedziane należy właściwie wprowadzić i zaterminować w panelach krosowych. Panele muszą charakteryzować się szeregiem własności funkcjonalnych oraz użytkowych pozwalających na sprawne, wygodne i oszczędne użytkowanie systemu okablowania przez cały okres jego eksploatacji:

- Panel musi zajmować maks.1U miejsca w szafie 19”
- Zagęszczenie portów musi zapewniać obsługę do 48 portów RJ45 lub min 96 włókien światłowodowych w przestrzeni 1U przy czym, skalowalność panela to 1 port
- Panel musi charakteryzować się budową modularną tj. obudowa musi być platformą zarówno dla złączy miedzianych (ekranowanych oraz nieekranowanych) jak i światłowodowych (W szczególności typu: SC, LC, E2000, FC, ST)
- Panel musi mieć możliwość jednoczesnego obsadzenia zarówno złączami miedzianymi jak i światłowodowymi
- Panel musi gwarantować obsługę łączy światłowodowych zakończonych różnego rodzaju kasetami światłowodowymi tj, typu breakout, pod spawy oraz typu MPO
- Pojedyńcza kaseta światłowodowa powinny obsługiwać pomiędzy 1 port a maksimum 12 portów
- Panel krosowy powinien obsługiwać do 8 kaset światłowodowych.

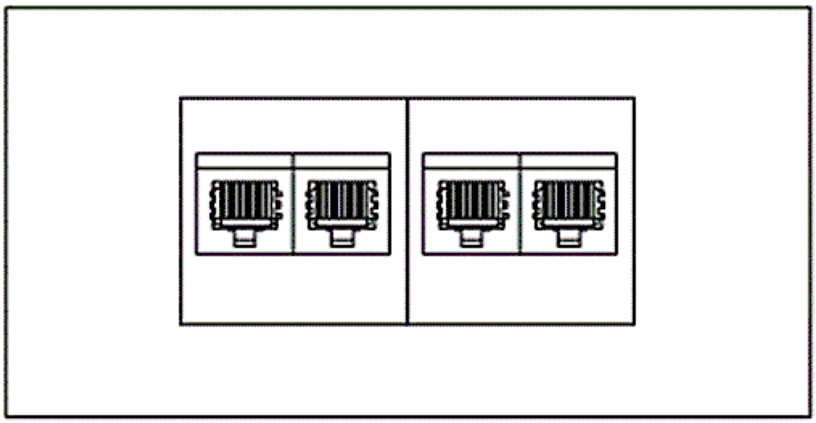
- Kasety światłowodowe bez względu na typ muszą w swojej konstrukcji zapewniać możliwość wykonania zapasu kabla/pigtaila, posiadać miejsce dedykowane do przytwierdzenia kabli wchodzących oraz opcjonalnie miejsce wykonania spawu – przymocowanie magazynku spawów do obudowy kasety.
- Kasety muszą charakteryzować się maksymalną elastycznością dając możliwość zmiany obsługiwanych złączy światłowodowych. Zmiana ta powinna być możliwa poprzez błyskawiczną wymianę płyty czołowej kasety (bez użycia narzędzi).
- Panel krosowy musi posiadać zintegrowaną półkę kablową umożliwiającą przytwierdzenie wprowadzonego kabla za pomocą elementów mocujących, co zabezpiecza moduły przyłączeniowe przed naprężeniem pochodzącym od kabla
- System w skład którego wchodzi panel musi umożliwiać kodowanie kolorem co poprawia walory administracyjne rozwiązania
- Panel musi mieć możliwość wyposażenia w organizator kabli krosowych, który nie wymagałaby zajęcia dodatkowej przestrzeni w szafie
-Panel musi być wyposażony w duże, widoczne i wygodne w użyciu etykiety połączeń w miejscu gdzie nie byłyby one zasłaniane przez wpięte kable krosowe
- Panel musi posiadać możliwość zaślepienia miejsc (slotów) w danej chwili nieużywanych. Zaślepki powinny dawać możliwość instalacji bez konieczności użycia jakichkolwiek narzędzi.



Rysunek 4. Panel krosowy 48 x RJ45 kat 6a FTP

3.1.1.5 Gniazda abonenckie

Gniazda Abonenckie (PEL) zaprojektowano w standardzie instalacyjnym Mosaic 45x45 /w wykonaniu natynkowym. Poszczególne PEL'e muszą zawierać 4 porty miedziane RJ45 o wydajności zgodnej z wydajnością projektowanego systemu. Płyta czołowa PEL dla adapterów miedzianych musi być płytą kątową co ułatwia użytkowanie gniazd. Gniazda muszą być wyposażone w widoczne pola opisowe zabezpieczone mechanicznie przed przypadkowym uszkodzeniem/zdarciem. Gniazdo musi być wyposażone w uchylne zaślepki przeciwkurzowe umożliwiające jednoczesne kodowanie kolorem co znacznie ułatwia użytkowanie, administrację oraz zmniejsza ryzyko wystąpienia błędnego połączenia.



Rysunek 5. Gniazda PEL: 4xRJ45 kat6 FTP

Rysunek 8. Adapter 45x45 oraz moduł keystone kat 6 FTP

3.1.2 PODSYSTEM OKABLOWANIA PIONOWEGO – POŁĄCZENIA ŚWIATŁOWODOWE

3.1.2.1 Światłowodowe okablowanie szkieletowe

3.1.2.1.1 Światłowodowy kabel szkieletowy

Wymaga się, aby producent dostarczanego systemu był również producentem kabli światłowodowych. Światłowodowe okablowanie pionowe będzie zrealizowane jako połączenie z istniejącą infrastruktura teletechniczną. Światłowodowy kabel instalacyjny musi cechować się szeregiem własności zarówno transmisyjnych jak i mechanicznych.Połączenia pomiędzy punktami GPD a istniejącym budynkiem mają być realizowane za pomocą preterminowanych kabli światłowodowych MM OM3. Na obu końcach muszą być zaterminowane złączami LC w kaskadzie podwójnej.

Rodzaj włókien	MM
Kategoria włókien	OM3
Ilość włókien	24
Szlif złącza	PC
Straty wtrąceniowe (IL), 100% zgodnie z IEC 61300-3-4	≤0,3 dB
Średnie straty wtrąceniowe (IL) zgodnie z IEC 61300-3-4	≤0,15 dB

Straty odbiciowe (RL) Zgodnie z IEC 61300-3-6	≥30 dB (MM PC)
Ilość cykli połączeniowych @ΔIL<0.2 dB	1000
Kolorystyka powłoki	szary
Max zewnętrzna średnica kabla	11.5 mm +/- 5%

Tabela 4. Wymagane właściwości dla kabla przyłączeniowego preterminowanego

3.1.2.2 Panele światłowodowe

Zastosowane panele światłowodowe powinny charakteryzować się jak najdalej posuniętą uniwersalnością i ergonomia użytkowania. W tym celu wymaga się aby panele spełniały następujące wymagania:

PRZEŁĄCZNICA ŚWIATŁOWODOWA 1U
- Przełącznica musi zajmować w przestrzeni szafy 19” nie więcej niż 1 jednostkę (1U)
- Maksymalna głębokość przełącznicy to 255 mm
- Przełącznica musi charakteryzować się konstrukcją modularną z pełnym wysuwem płyty czołowej na szynach teleskopowych
- Przełącznice światłowodowe w swojej przestrzeni muszą być wyposażone w perforacje wewnętrzne mające na celu zarządzanie tubami lub włóknami światłowodowymi
- Konstrukcja przełącznic powinna być maksymalnie uniwersalna tj. wymaga się aby dla rozwiązań spawanych i pre-terminowanych znajdował zastosowanie de-facto jeden rodzaj przełącznicy różniący się jedynie wyposażeniem
- Płyta czołowa przełącznicy musi umożliwiać w dowolnym momencie eksploatacji migrację na dowolny typ obsługiwanych złączy bez konieczności wymiany całych przełącznic
- Płyta czołowa przełącznicy musi mieć możliwość zatrzaskiwanego montażu adapterów światłowodowych
- W projekcie założono możliwość zakończenia w przełącznicy do 24F włókien światłowodowych w przestrzeni pojedynczej jednostki (1U) zakończonych adapterem typu LC DX,
- Przełącznica musi mieć możliwość doposażenia w organizator patchcordów światłowodowych występujący jako półka przednia, zintegrowany z przełącznicą w ramach 1U. Organizator ten musi mieć taka konstrukcje, aby jednocześnie zapewnić ochronę patchcordów przed nadmiernymi naprężeniam i/lub mechanicznym uszkodzeniem na skutek np. przytrzaśnięcia przez drzwi szafy
- Przełącza musi być wyposażona w uchwyt na element siłowy kabla oraz mieć regulowane uchwyty boczne, co umożliwi przesuwanie przełącznicy w głąb szafy
- Przełącznice muszą stanowić kompletne rozwiązanie gotowe do instalacji i ułożenia kabli wewnątrz przełącznicy. W skład takiego kompletu muszą wejść:

WERSJA PRETERMINOWANA
- Płyta czołowa umożliwiająca montaż odpowiednich adapterów światłowodowych i odpowiedniej ilości potrzebnych włókien
- komplet adapterów połączeniowych

3.1.2.3 Wyposażenie optyczne gniazd abonenckich oraz paneli krosowych

Opisane powyżej wymagania dotyczące paneli krosowych oraz gniazd abonenckich dotyczyły oczekiwanej funkcjonalności platform dla światłowodowych systemów transmisyjnych. Poniżej zebrano wymagania transmisyjne dotyczące światłowodowego osprzętu połączeniowego

3.1.2.3.1 Adaptery światłowodowe

Adaptery światłowodowe będące na wyposażeniu platform opisanych powyżej powinny charakteryzować się następującymi własnościami:
- Zewnętrzny korpus adaptera musi być wykonany w technologii jednolitego odlewu, co poprawia właściwości mechaniczne adaptera i eliminuje rozpad adaptera na dwie części
- Tuleje centrujące będące częścią zastosowanych adapterów FO przeznaczone do transmisji SM powinny być ceramiczne co poprawia mechaniczne własności adaptera (niezawodność, dwukrotnie większa żywotność) oraz poprawia własności optyczne całego połączenia.

- Adaptery powinny pracować w zakresie temperaturowym -40 do +85 ^{O}C i zapewniać w tym zakresie temperaturowym właściwe parametry optyczne toru światłowodowego
- Ze względów bezpieczeństwa, adaptery muszą być wyposażone w automatyczne przesłony zewnętrzne lub wewnętrzne chroniące wzrok przed promieniowaniem laserowym LC.
- Adaptery światłowodowe muszą być wyposażone zaślepki przeciwkurzowe.
- Kolorystyka adapterów połączeniowych będących na wyposażeniu przełącznic ma umożliwiać identyfikację kabli światłowodowych:

Dla wielomodowych PC aqua

3.1.2.3.2 Złącza światłowodowe (pigtaile, kable krosowe, kable szkieletowe)

Złącza światłowodowe mające zastosowanie w pigtailach, pre-terminowanych kablach połączeniowych oraz kablach krosowych mają decydujący wpływ na parametry transmisyjne całego łącza a co za tym idzie decydują czy łącza światłowodowe są w stanie obsłużyć żądane przez użytkownika aplikacje czy tez nie. Z tego powodu elementy te stanowiące kluczową część wymienionego powyżej asortymentu musza spełniać najsurowsze wymagania dotyczące konstrukcji oraz parametrów transmisyjnych:
- Na potrzeby niniejszego projektu wymaga się zastosowania w całej sieci złączy typu LC, w wersjach SM.
- Ferule złączy powinny być ceramiczne co poprawia mechaniczne własności połączenia (niezawodność, dwukrotnie większa żywotność) oraz poprawia własności optyczne całego połączenia
- Ferrule wtykow PC muszą mieć koncentryczność < 1 µm,
- Ferrule muszą charakteryzować się szlifem czoła ferruli PC/APC
- złącza muszą być wyposażone w odgiętki stanowiące zabezpieczenie złączy przed zbyt małymi promieniami gięcia.
- Złącza światłowodowe muszą charakteryzować się następującymi parametrami transmisyjnymi:

Złącza wielomodowe MM

Średnie straty wtrąceniowe IL [dB] zgodnie z IEC 61300-3-34	≤0.12 dB
Średnie straty odbiciowe RL [dB] zgodnie z IEC 61300-3-6	35 dB @ PC MM

3.1.2.3.3 Światłowodowe kable krosowe

Zakłada się użycie światłowodowych kabli krosowych SM. Kable muszą być zakończone złączem LC duplex. Wymaga się stosowania kabli krosowych o długościach 2m. Kable krosowe muszą być wykonane na włóknach G.652D/OS2.
Światłowodowe kable krosowe muszą być wykonane na kablu patchcordowym o średnicy zewnętrznej max 3,0 mm. Kable musza być wzmocnione kevlarem, co pozwala zachować wymagania mechaniczne wg normy GR 326(@Media 1)
Parametry złączy: patrz punkt 5.1.2.3.2

3.1.2.3.4 Pigtaile światlowodowe

Zaklada się użycie pigtaili światłowodowych SM. Musza one być zakończone złączem LC. Wymaga się stosowania pigtaili o długościach min 2m. Pigtaile muszą być wykonane na włóknach G.652D/OS2. Pigtaile zainstalowane w panelach krosowych musza być wykonane w 12 kolorowej palecie kolorów zgodnie z IEC 60304. Parametry złączy patrz punkt 5.1.2.3.2

3.1.3 WYPOSAŻENIE GPD

Punkty dystrybucyjne powinny być zrealizowane w oparciu o skręcane szafy teleinformatyczne w standardzie 19”.

Szafy musza być wyraźnie oznaczone logiem producenta systemu okablowania strukturalnego, i stanowić integralny element systemu. Drzwi przednie i tylne jednoskrzydłowe perforowane 80%. Kolor czarny, konstrukcja skręcana, nośność 1500kg.
Zakłada się wyposażenie szaf w :

- Zestaw wentylatorów dachowo-podłogowych
- Listwy zasilające
- Zabezpieczenia przepustów kablowych
- Półki regulowane

W GPD zostaną zainstalowana szafa w rozmiarze 33U 600x600

Rysunek 7. Szafa serwerowa stojąca 33U 600x600

4. PRZYKŁADOWE ZESTAWIENIE MATERIAŁÓW

LP	Materiał		
	Punkty dystrybucyjne	**j.m.**	**SUMA**
1	SZAFA RAMOWA STOJĄCA, 33U/600/600 DRZWI BLACHA/SZKŁO, TYŁ BLACHA PEŁNA, SKRÓCONY RAL 9005 (KONSTRUKCJA SKRĘCANA - NOŚNOŚĆ 1000 KG)	szt.	**1**
2	COKÓŁ 100 MM, DO SZAFY O SZER 600 I GŁĘB 600 MM, ŚCIANY COKOŁU PEŁNE RAL 9005	szt.	**1**
3	PANEL WENTYLACYJNY 4-WENTYLATOROWY DACHOWO-PODŁOGOWY Z TERMOSTATEM 1HE RAL 9005	szt.	**1**
4	LISTWA ZASILAJĄCA 19" 9 GNIAZD Z BOLCEM, WTYK UNISCHUKO	szt.	**1**
5	LISTWA UZIEMIAJĄCA MIEDZIANA 9 X M6 DL.220MM	szt.	**1**
6	PRZEŁĄCZNICA TELESKOPOWA 1U 19" NIEWYPOSAŻONA 255MM RAL9005 CZARNA	szt.	**3**
7	PŁYTA CZOŁOWA 1U 12XSC SIMPLEX, MTRJ,E2000,LC CZARNA	szt.	**2**
8	PŁYTA CZOŁOWA 1U 24XSC SIMPLEX, MTRJ,E2000,LC CZARNA	szt.	**1**
9	ADAPTER LC/PC MM, DX, STANDARD, CERAMICZNA TULEJA, PLASTIKOWA OBUDOWA, FLANSZA, AQUA	szt.	**48**

10	PRE-CONNECTORIZED EXO-G0 100M 24G 50/125 OM3 MM 24LC/24LC EASYLINK1	szt.	**1**
11	PRE-CONNECTORIZED EXO-G0 25M 24G 50/125 OM3 MM 24LC/24LC EASYLINK1	szt.	**1**
12	Panel krosowy niewyposażony, z uziemieniem, 8 slotów	szt.	**5**
13	UCHWYT DO PRZEŁACZNICY HD POD MODUŁU PRZYŁĄCZENIOWE 6XRJ45/S, NIEWYPOSAŻONY	szt.	**39**
14	Moduł kategorii 6, ekranowany	szt.	**232**
15	LISTEK OPISOWY DO PRZEŁĄCZNICY HD	szt.	**39**
16	ORGANIZATOR POZIOMY KABLI 19" - Z ZAMYKANYMI PLASTIKOWYMI USZAMI CZARNY RAL9005 1U	szt.	**15**
17	PÓŁKA STAŁA 19", 1U, O GŁ. 350 MM., MOCOWANA W CZTERECH PUNKTACH RAL 9005	szt.	**8**
18	KOMPLET ŚRUB MONTAŻOWYCH (20X ŚRUBA M6X16 + PODKŁADKA + NAKRETKA KOSZYKOWA)	kpl.	**4**
LP	**Okablowanie pionowe i poziome + kable krosowe**	**j.m.**	**SUMA**
19	DATA KABEL INSTALACYJNY CAT.6 U/FTP 4PR LSZH CPR CLASS DCA 400 MHZ 500MB NIEBIESKI	m	**10000**
20	PATCHCORD 2M LC/LC OM3 2,8MM DUPLEX GOLD	szt.	**2**
21	PATCHCORD 1M LC/LC OM3 2,8 DUPLEX GOLD	szt.	**5**
22	DATA PATCHCORD CAT. 6A S/FTP, 2 M, SZARY KABEL, WTYK TURKUSOWY, BOOT CZARNY TR., IKONA ZIELONA, ODGIĘTKA CZARNA TR.	szt.	**232**
LP	**Gniazdo LAN**	**j.m.**	**SUMA**
23	Moduł przyłączeniowy HD RJ45 kategorii 6, ekranowany	szt.	**232**
24	EM 45 PUSZKA N/T 4MOD	szt.	**58**
25	EM SUPORT 4MOD	szt.	**58**
26	EM RAMKA 4MOD	szt.	**58**
27	ADAPTER 45 X 45 MM POD 2 MODUŁY KEYSTONE	szt.	**116**
28	SFP+ 10GBASE-SR ETHERNET 850NM MMF 300M 10GBPS LC DUPLEX DDMI	szt.	**4**

5. ADMINISTRACJA

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, tak od strony gniazda, jak i od strony szafy montażowej zgodnie ze standardem TIA-606-B oraz ISO/IEC TR14763-2-1. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach.
Powykonawczo należy sporządzić dokumentację instalacji kablowej zawierającej trasy kablowe i rozmieszczenie punktów przyłączeniowych w pomieszczeniach zgodnie ze stanem rzeczywistym. Do dokumentacji należy dołączyć raporty z pomiarów torów sygnałowych

6. GWARANCJA

Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta, obejmującą całą część transmisyjną wraz z kablami krosowymi i innymi elementami dodatkowymi. Gwarancja ma być udzielona przez producenta bezpośrednio klientowi końcowemu.

25-letnia gwarancja systemowa ma być bezpłatną usługą serwisową oferowaną użytkownikowi końcowemu (inwestorowi) przez producenta okablowania. Musi obejmować ona swoim zakresem całość systemu okablowania od głównego punktu dystrybucyjnego do gniazda użytkownika i zawierać, podsystem okablowania szkieletowego i poziomego. W celu uzyskania tego rodzaju gwarancji cały system musi być zainstalowany przez firmę instalacyjną posiadającą odpowiedni status uprawniający do udzielenia gwarancji producenta. Wniosek o udzielenie gwarancji składany przez firmę instalacyjną do producenta ma zawierać: listę zainstalowanych elementów systemu, wyciąg z dokumentacji powykonawczej podpisany przez projektanta oraz instalatora, wyniki pomiarów dynamicznych typu Permanent Link wszystkich torów transmisyjnych według norm ISO/IEC

11801 ed. 2.2 lub EN 50173-1. Aby na etapie oferty dowieść zdolności udzielenia gwarancji 25-letniej systemowej producenta systemu okablowania – użytkownikowi końcowemu (lub Inwestorowi) firma instalacyjna winna przedstawić: - certyfikat imienny zatrudnionego pracownika wydany przez producenta (a nie w imieniu producenta).

7. ODBIORY

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganymi przez niniejszy Projekt wydajnościami określonymi w normach referencyjnych ujętych w punkcie 3.2.2. niniejszego opracowania.
W celu odbioru instalacji okablowania strukturalnego należy spełnić następujące
warunki:

1) Instalacja

Instalacja musi być wykonana zgodnie z wytycznymi producenta okablowania strukturalnego oraz wytycznymi norm referencyjnych wskazanymi w punkcie 3, w szczególności:
• EN 50174-1:2009/A1:2011 Information Technology - Cabling system installation- Part 1. Specification and quality assurance
Wraz z jej polskim odpowiednikiem:
PN-EN 50174-1:2010/A1:2011 Technika informatyczna - Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości
• EN 50174-2:2009/AB2013 Information Technology - Cabling system installation - Part 2. Installation planning and practices internal to buildings
Wraz z jej polskim odpowiednikiem:
PN-EN 50174-2:2010/A1:2011 Technika informatyczna - Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków
• EN 50174-3:2013 Information Technology - Cabling system installation - Part 3. – Industrial premises
Wraz z jej polskim odpowiednikiem:
PN-EN 50174-3:2014-02E Technika informatyczna - Instalacja okablowania - Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków
• EN 50310:2010 Application of equipotential bonding and earthling at premises with information technology equipment.
Wraz z jej polskim odpowiednikiem:
PN-EN 50310:2012 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym

2) Pomiary sieci

Pomiary należy wykonać zgodnie z wymaganiami producenta okablowania strukturalnego oraz norm referencyjnych wykazanych w punkcie 3.2.2. a w szczególności:
• EN 50346:2002/A1:2007/A2:2009 Information Technology - Cabling system installation - Testing of installed cabling
Wraz z jej polskim odpowiednikiem:
PN-EN 50346:2004/A1:202009/A2:2010 Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania
• EN 61935-1:2009 Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards
Wraz z jej polskim odpowiednikiem:
PN-EN 61935-1:2010E Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii telekomunikacyjnych -- Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm EN 50173
• ISO/IEC 14763-3:2006/A1:2009 Information technology –Implementation and operation of customer premises cabling – Part 3: Testing of optical fibre cabling

Wraz z jej polskim odpowiednikiem:
PN-ISO/IEC 14763-3:2009/A1:2010P Technika informatyczna - Implementacja i obsługa okablowania w zabudowaniach użytkowych - Część 3: Testowanie okablowania światłowodowego
Mierniki użyte w procesie pomiarowym muszą uzyskać aprobatę producenta systemu okablowania.

3) Wykonanie dokumentacji powykonawczej

Dokumentacja powykonawcza musi zostać wykonana i przekazana Inwestorowi. Musi ona zawierać:
- Raporty z pomiarów dynamicznych okablowania,
- Rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych
- Oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych
- Lokalizację przebić przez ściany i podłogi.
- Raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji. Drugą kopię pomiarów (dokumentacji powykonawczej) należy przekazać producentowi okablowania w celu udzielenia inwestorowi (Użytkownikowi końcowemu) bezpłatnej gwarancji.

II. Urządzenia aktywne – minimalne parametry:

Switch zarządzalny do gniazd klienckich – 5 szt. :

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

- Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
- Chłodzenie od przodu do tyłu obudowy
- Możliwość instalacji redundantnego zasilacza
- Tablica MAC min. 16K
- Tablica ARP/NDP min. 888
- Bufor 16Mb
- MTBF min. 578472 godzin
- Wydajność min. 130,9 Mp/s
- Przepustowość min. 176 Gb/s
- Port USB
- Port miniUSB
- Port zarządzania Out-of-band;
- Web GUI
- HTTPs
- CLI
- Telnet
- SSH
- SNMP
- MIB RSPAN
- Radius
- TACACS+
- DiffServ

- Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
- IPv4/IPv6 Multicast filtering
- IGMPv3 MLDv2 Snooping
- ASM & SSM
- IGMPv1,v2 Querier
- Auto-VoIP
- Auto-iSCSI
- Policy-based routing (PBR)
- LLDP-MED
- Spanning Tree
- Green Ethernet
- STP
- MTP
- RSTP
- PV(R)STP
- BPDU/STRG Root Guard
- EEE (802.3az)
- GVRP/GMRP
- Q in Q,
- Private VLAN
- DOT1X
- MAB
- Captive Portal
- DHCP Snooping
- Dynamic ARP
- Inspection
- IP Source Guard
- CPU min 800 Mhz
- Min 1GB RAM
- Min 256MB Flash
- Min ilość obsługiwanych VLAN 4K
- DHCP Server min 2K rezerwacji
- sFlow
- Minimalna ilość przełączników w stosie: 8
- Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
- Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
- Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
- Non-stop forwarding (NSF)
- Distributed Link Aggregation (LAGs across the stack)
- Ilość interfejsów IP 128
- Double VLAN Tagging (QoQ)
- PIM-DM (Multicast Routing - dense mode)
- PIM-DM (IPv6)
- PIM-SM (Multicast Routing - sparse mode)
- PIM-SM (IPv6)
- RIPv1
- RIPv2
- OSPFv2
- RFC 2328

- RFC 1583
- OSPFv3
- OSPFv2 min. sąsiadów 400
- OSPFv3 min. sąsiadów 400
- OSPFv3 min. sąsiadów na interfejs 100
- UDLD
- LLPF
- DHCPv6 Snooping
- wysyłanie alertów na email
- MMRP
- Ilość ACL min. 100
- Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
- Zasilacz z certyfikatem 80+
- CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
- Class A, EN 61000-3-3:2013, EN 55024:2010
- VCCI : VCCI-CISPR 32:2016, Class A
- RCM: AS/NZS CISPR 32:2013 Class A
- FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
- ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
- BSMI: CNS 13438 Class A

W przypadku użycia w niniejszej Specyfikacji Technicznej nazw własnych, Zamawiający dopuszcza rozwiązania równoważne.

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 2 do Warunków

Specyfikacja Techniczna dotycząca System nr 2 - specjalistyczne oprogramowania do zabezpieczenia 232 komputerów podczas egzaminu, licencje bezterminowe, systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożeń. Celem zabezpieczenia komputerów podczas zdawania egzaminów w systemie SBS niezbędny jest zakup specjalistycznego oprogramowania, które zostanie zainstalowane na każdym z 232 komputerów. Oprogramowanie to uniemożliwi utworzenie odpowiednich polityk zabezpieczeń, które spowodują, że podczas egzaminu student będzie miał dostęp tylko i wyłącznie do stron Uczelni przeznaczonych do zdawania egzaminów. Natomiast pozostałe strony internetowy oraz zasoby Uczelni z materiałami dydaktycznymi zostaną zablokowane na czas egzaminu. Oprogramowanie zabezpieczające posłuży również do zablokowania dostępu do dysku komputera Studentowi zdającemu egzamin, a także do napędu CD/DVD oraz portów USB.

Zakup specjalistycznego oprogramowania do zabezpieczeń

Wymagana jest dostarczenie licencji dostępowych (CAL) do 232 zestawów komputerowych – licencja musi zapewnić możliwość podłączenie do pracy w domenie Active Directory.

Oprogramowanie do zabezpieczenia – 232 zestawów komputerowych:
Ochrona stacji roboczych - Windows
1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.
6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.
Ochrona antywirusowa i antyspyware
7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
9. Wbudowana technologia do ochrony przed rootkitami.
10. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
12. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.

13. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
14. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
15. Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
16. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
17. Możliwość skanowania dysków sieciowych i dysków przenośnych.
18. Skanowanie plików spakowanych i skompresowanych.
19. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
37. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
40. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
43. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
45. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
46. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
47. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

48. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
51. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
52. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
53. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
54. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
55. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
57. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
58. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
59. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
60. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
61. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
62. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

63. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
64. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
65. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
• tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
• tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
• tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
66. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
67. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
68. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
69. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
70. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
71. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
72. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
73. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
74. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
75. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.

76. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
77. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
78. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
79. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
81. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
82. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
83. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
85. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
86. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
87. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
88. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
89. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
90. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
91. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
92. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
93. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

94. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
95. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
96. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
97. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
98. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
99. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
100. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
101. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
102. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
103. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
104. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
105. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
106. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
107. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
108. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
109. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona przed spamem

110. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
111. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.

112. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
113. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
114. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
115. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
116. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
117. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
118. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
119. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
120. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
Zapora osobista (personal firewall)
121. Zapora osobista ma pracować w jednym z czterech trybów:
• tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
122. Program musi oceniać reguły zapory systemu Windows.
123. Możliwość tworzenia list sieci zaufanych.
124. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
125. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
126. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
127. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
128. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
129. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.

130. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
131. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
132. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
133. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
134. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
135. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
136. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
• z aplikacją lokalną, którą administrator wskazuje z listy,
• z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.
Kontrola dostępu do stron internetowych
137. Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.
138. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
139. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
140. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy,
nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
141. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
142. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
143. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.

144. Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
145. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.
Bezpieczna przeglądarka
146. Aplikacja musi być wyposażona w moduł bezpiecznej przeglądarki.
147. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
148. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
149. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
150. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
151. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
Stacje Robocze Apple Mac OS X
1. Pełne wsparcie dla systemów Mac OS X 10.12 lub nowszych.
2. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
3. Pomoc w programie (help) w języku polskim oraz angielskim.
4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
7. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

14. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
16. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
17. Możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.
18. Aktualizacje modułów analizy heurystycznej.
19. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
20. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
21. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
22. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
23. Ochrona przed atakami typu „phishing”.
24. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.
25. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
26. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).
29. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
30. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

31. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.
32. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
33. Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.
34. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.
35. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.
36. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
37. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej.
38. Ochrona poczty mail:
• Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego.
• Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
• Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
• Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
• Możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.
• Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
39. Zapora osobista
• Zapora osobista może pracować jednym z 2 trybów:
o Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
o Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
• Możliwość dezaktywacji funkcji zapory sieciowej.
• Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
• Możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
• Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.

• Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.
• Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
• Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
• Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
• Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
• Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, Sieć WiFi, Podsieć IPv4/IPv6, Zakres adresów IPv4/IPv6, Adres IPv4/IPv6.
40. Kontrola dostępu do stron internetowych
• Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
• Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
• Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
• Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
• Aplikacja musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
• Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
• Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
• Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.
Stacje robocze Linux
1. Produkt musi wspierać systemy operacyjne Ubuntu Desktop 18.04 / 20.04 LTS 64-bit, Red Hat Enterprise Linux 7 64-bit, SUSE Linux Enterprise Desktop.
2. Produkt musi posiadać obsługę środowisk pulpitu GNOME,KDE,XFCE.
3. Produkt musi posiadać wsparcie dla dystrybucji 64-bitowych.
4. Pomoc produktu musi być w języku polskim oraz angielskim.
5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
7. Wbudowana technologia do ochrony przed rootkitami.
8. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
10. Skanowanie plików spakowanych i skompresowanych.
11. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
13. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
14. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
15. Aktualizacje modułów analizy heurystycznej.
16. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
17. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
18. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
19. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
20. Aktualizacja systemu antywirusowego ma być dostępna z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
21. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
22. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
23. Program ma umożliwiać importowanie oraz eksportowanie ustawień lokalnie oraz zdalnie za pomocą dedykowanego narzędzia.
24. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona urządzeń mobilnych opartych o system Android

1. Wspierany system co najmniej Android 5.0.

2. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Procesor: ARM z obsługą ARMv7 lub x86 Intel Atom.

Ochrona antywirusowa:

4. Ochrona plików w czasie rzeczywistym.
5. Ochrona przed atakami typu „phishing".
6. Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
8. Ochrona proaktywna wykrywająca nieznane zagrożenia.
9. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
10. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
11. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

12. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Ochrona przed kradzieżą:

16. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
17. Dodanie zaufanej karty SIM ma się odbyć w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o wprowadzony ręcznie numer IMSI karty SIM.
18. W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,
b. przywrócenie urządzenie do ustawień fabrycznych,
c. zablokowania urządzenia,
d. uruchomienie sygnału dźwiękowego,
e. lokalizację GPS.

Polityka ustawień:

19. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:

a. połączenie Wi-Fi,
b. GPS,
c. usługi lokalizacyjne,
d. pamięć,
e. roaming danych,
f. roaming połączeń,

g. nieznane źródła,
h. tryb debugowania,
i. komunikacja NFC,
j. szyfrowanie pamięci masowej,
k. urządzenie zrootowane.

Kontrola aplikacji:

20. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
21. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
22. Blokowanie aplikacji musi być możliwe w oparciu o:
a. nazwę aplikacji,
b. nazwę pakietu,
c. kategorię sklepu Google Play,
d. uprawnienia aplikacji,
e. pochodzenie aplikacji z nieznanego źródła.

Zabezpieczenia urządzenia:

23. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
a. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
b. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
d. czas, po którym automatycznie nastąpi blokada ekranu,
e. ograniczenie dostępu do kamery wbudowanej w urządzenie.

Aktualizacje sygnatur:

24. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
25. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
26. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:

27. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
28. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
29. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
30. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.

31. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:
a. za pomocą kodu QR,
b. za pomocą unikatowego łącza,
c. za pomocą wiadomości e-mail,
32. W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).

Administracja zdalna

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.

20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
29. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
30. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
31. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
32. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
33. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
34. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
35. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz

wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.

36. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.

37. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.

38. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.

39. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

40. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.

41. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.

42. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.

43. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

44. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

45. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.

46. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.

47. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.

48. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.

49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.

50. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
51. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
52. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
53. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
54. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
55. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
56. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
57. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
58. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
60. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
61. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
62. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
63. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
64. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
65. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
66. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.

67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
68. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
69. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.
70. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
71. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
72. Powiadomienia mailowe mają być wysyłane w formacie HTML.
73. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
74. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
75. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
76. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
77. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
78. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
79. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
80. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
81. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
82. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
83. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
84. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak:

antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.

85. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.

86. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.

87. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.

88. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.

89. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.

90. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.

91. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).

92. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.

93. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).

94. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

System bezpieczeństwa – minimalne wymagania:

- Licencja dostarczona na 10 aktywnych urządzeń z możliwością rozbudowy.
- skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
- interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
- jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
- serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
- liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
- działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
- liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
- kompilator plików MIB
- obsługa pułapek SNMP
- routery i switche: mapowanie portów
- obsługa komunikatów syslog

- alarmy zdarzenie - akcja
- powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)
- raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)
- audyt inwentaryzacji sprzętu i oprogramowania
- wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
- zdalny dostęp do managera plików z możliwością usuwania plików użytkownika
- informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej
- szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
- zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI
- alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
- lista kluczy oprogramowania Microsoft
- aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR
- możliwość archiwizacji i porównywania audytów
- monitorowanie harmonogramu zadań Windows
- minimalizacja zjawiska cyberslackingu i zwiększenie wydajności pracowników
- redukcja kosztów wydruku
- blokowanie stron WWW
- blokowanie uruchamianych aplikacji
- monitorowanie wiadomości e-mail (nagłówki) - antyphishing
- szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)
- użytkowane aplikacje (aktywnie i nieaktywnie)
- odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
- audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
- użycie łącza: generowany przez użytkowników ruch sieciowy
- statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
- zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)
- zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami
- informacje o urządzeniach podłączonych do danego komputera
- lista wszystkich urządzeń podłączonych do komputerów w sieci
- audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych
- zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników
- centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory
- integracja bazy użytkowników i grup z Active Directory
- alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym
- lista aplikacji używanych przez pracowników z rozbudowaną możliwością filtrowania, przypisywania do wybranych kategorii i nadawania im odpowiednich statusów
- podgląd aplikacji używanych w grupie bądź przez indywidualnego użytkownika w dowolnym czasie
- dodawanie wyjątków przez administratora grupy, wskazujących, że dana aplikacja w tej grupie jest uznawana za produktywną
- możliwość wskazywania przez administratora statusów konkretnych aplikacji: produktywna / neutralna / nieproduktywna
- grupowanie stron internetowych oraz aplikacji z podziałem na: produktywne / nieproduktywne / neutralne
- widok najczęściej używanych aplikacji produktywnych, nieproduktywnych i neutralnych w dowolnie wybranym okresie czasu

- definiowanie minimalnego progu produktywności (czasu spędzonego w aplikacjach produktywnych) i maksymalnego progu nieproduktywności (czasu spędzonego w aplikacjach nieproduktywnych)
- cykliczne alerty wysyłane mailem o przekroczeniu zdefiniowanych progów produktywności
- możliwość ustalania okresu, po którym dane mają być usuwane z modułu SmartTime
- lista kontaktów w organizacji z wbudowaną wyszukiwarką
- podgląd zrzutu ekranu wybranego użytkownika dostępny dla menedżerów i administratorów

W przypadku użycia w niniejszej Specyfikacji Technicznej nazw własnych, Zamawiający dopuszcza rozwiązania równoważne.

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 3 do Warunków

FORMULARZ OFERTOWY

I. Dane dotyczące Wykonawcy:

nazwa: .....

siedziba: .....

strona internetowa: .....
numer telefonu: .....
adres e-mail: ....
numer REGON: .....
numer NIP: .....

II. Dane dotyczące Zamawiającego:

WSPiA Rzeszowska Szkoła Wyższa
ul. Cegielniana 14
35-310 Rzeszów
numer REGON: 650162512
numer NIP: 795-10-56-506
strona internetowa: www.wspia.eu

III. Adres do korespondencji:
Marek Rogalski
WSPiA Rzeszowska Szkoła Wyższa
ul. Cegielniana 14
35-310 Rzeszów, budynek „A" I piętro, pok. 1.02

numer telefonu: (17) 867 04 46
adres e-mail: marek.rogalski@wspia.eu

IV. Zobowiązania i oświadczenia Wykonawcy:

1. Nawiązując do ogłoszenia zapytania ofertowego numer 8/KON/z045/2021 w ramach którego sprecyzowane zostały Warunki zamówienia na zakup urządzeń, sprzętu i oprogramowania wraz z ich instalacją i wdrożeniem – jako wsparcie informatycznych narzędzi zarządzania WSPiA - w celu dostosowania jakości kształcenia w Uczelni obejmujących:
   1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;

2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;

- oferujemy wykonanie przedmiotu zapytania ofertowego, zgodnie z wymogami niniejszych Warunków za cenę:

	Cena netto	Podatek VAT	**Cena brutto**
System nr 1 – wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej wraz z ich instalacją i wdrożeniem			
System nr 2 – specjalistyczne oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu, licencje bezterminowe, systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożenia (zgodnie z Umową określoną w ust. 12);			
Łączna cena przedmiotu zamówienia - System nr 1 + System nr 2			

2. **Oświadczamy, że:**
1) zapoznałem się i akceptuję Warunki realizacji zamówienia określone w zapytaniu ofertowym, nie wnoszę żadnych zastrzeżeń i uwag w tym zakresie oraz uzyskałem niezbędne informacje do przygotowania oferty.
2) wykonam przedmiot zamówienia w terminie do dnia:…….
3) udzielę gwarancji – zgodnie z Załącznikiem nr 8 – na **36 miesięcy**, licząc od dnia dokonania bezusterkowego odbioru końcowego przedmiotu Umowy.
4) wady przedmiotu Umowy będą usuwane w terminach określonych w Umowie.
5) załączony do Warunków zamówienia wzór Umowy akceptuję bez zastrzeżeń i zobowiązuje się w przypadku wyboru mojej oferty do zawarcia Umowy zgodnie z tym wzorem, w miejscu i terminie wyznaczonym przez Zamawiającego.
6) zobowiązuje się do wniesienia zabezpieczenia należytego wykonania Umowy w wysokości:……., w formie:……

V. Dokumenty załączone do oferty:

Na potwierdzenie spełnienia warunków udziału w postępowaniu, do oferty załączamy:

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

VI. Zastrzeżenie Wykonawcy o tajemnicy przedsiębiorcy:
Informacje o tajemnicy przedsiębiorstwa.:
……

VII. Osoby ze strony Wykonawcy do kontaktów z Zamawiającym:

Osoba / osoby do kontaktów z Zamawiającym:
…… …… …… …… …… …… …… …… …… tel. kontaktowy, adres e-mail: …… …… ……do reprezentowania w postępowaniu
…… …… …… …… …… …… …… …… …… tel. kontaktowy, adres e-mail: …… …… …… do reprezentowania w postępowaniu

VIII. Pełnomocnik w przypadku składania oferty wspólnej:

Nazwa (firma) ……
Telefon…… adres e-mail: ……..
Zakres*:
- do reprezentowania w postępowaniu
- do reprezentowania w postępowaniu i zawarcia Umowy
- do zawarcia Umowy

IX. Inne informacje Wykonawcy:
……
……
……
……

……
(data i podpis uprawnionego przedstawiciela Wykonawcy)
* niepotrzebne skreślić

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 4 do Warunków

OŚWIADCZENIE WYKONAWCY
O BRAKU POWIĄZAŃ OSOBOWYCH
I KAPITAŁOWYCH Z ZAMAWIAJĄCYM

Oświadczam(my), że nie podlegam(my) wykluczeniu z postępowania o udzielenie zamówienia na podstawie zapisu zawartego w **podrozdziale 6.5.2 „Zasada konkurencyjności" pkt 2 lit. a** Wytycznych Ministerstwa Rozwoju w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 z dnia 22 sierpnia 2019 roku, 21 grudnia 2020 roku, MIiR/2014-2020/12(5) (z wyjątkami o których mowa w powołanym wyżej zapisie Wytycznych)

Oświadczam(my), że:

1) nie jestem/jesteśmy powiązany(i) osobowo, ani kapitałowo z Zamawiającym w rozumienia zapisu zawartego w **podrozdziale 6.5.2 „Zasada konkurencyjności" pkt 2 lit. a** ww. Wytycznych z którego wynika, że:

„Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu zamawiającego lub osobami wykonującymi w imieniu zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
b) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez IZPO,
c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli."

2) Nie jestem/jesteśmy powiązany(i) z Zamawiającym w żaden inny sposób niż wskazany w pkt 1).

.....
(data, pieczęć i podpis osoby uprawnionej do składania oświadczeń woli w imieniu Wykonawcy)

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 5 do Warunków

OŚWIADCZENIE ZŁOŻONE
W CELU WYKAZANIA SPEŁNIENIA WARUNKÓW,
O KTÓRYCH MOWA W CZĘŚCI X ust. 3 pkt. 3.1, pkt. 3.2., pkt. 3.3. WARUNKÓW

Oświadczam(my), że na dzień składania oferty:

1) Posiadam/my uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień.
2) Znajduje się/Znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia we wskazanych terminach.
3) Posiadam/my niezbędną wiedzę oraz dysponuję/dysponujemy odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania zamówienia

.....
(data, pieczęć i podpis osoby/osób uprawnionej/uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 6 do Warunków

OŚWIADCZENIE ZŁOŻONE
W CELU WYKAZANIA SPEŁNIENIA WARUNKÓW,
O KTÓRYCH MOWA W CZĘŚCI X ust. 3 pkt. 3.4 WARUNKÓW

Nazwa Wykonawcy .....

Adres Wykonawcy .....

Wykaz wykonanych instalacji i dostarczonego wyposażenia w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy niż 3 lata – w okresie prowadzenia działalności tj.:. jedna instalacja logiczna na minimum 50 przyłączy komputerowych – z podaniem daty i miejsca ich wykonania wraz z załączeniem dokumentów potwierdzających, że powyższe zadania zostały wykonane i ukończone prawidłowo.

Wykaz wymagany w celu potwierdzenia, że Wykonawca posiada niezbędną wiedzę oraz doświadczenie do wykonania przedmiotu zamówienia.

Lp.	**Inwestor/ Miejsce wykonania zadania**	**Zakres przedmiotowy zadania (rodzaj zadania)**	**Data rozpoczęcia / zakończenia zadania**
1			
2			
3			

Do wykazu należy dołączyć dokumenty potwierdzające, że zadnia te zostały wykonane i ukończone prawidłowo (np. listy referencyjne).

.....
(data, pieczęć i podpis osoby/osób uprawnionej/uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 7 do Warunków

KLAUZULA INFORMACYJNA ZAMAWIAJĄCEGO

Dotyczy: Zapytania ofertowego na zakup urządzeń, sprzętu i oprogramowania wraz z ich instalacją i wdrożeniem – jako wsparcie informatycznych narzędzi zarządzania WSPiA- w celu dostosowania jakości kształcenia w Uczelni obejmujących:

1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;

w ramach projektu pn.:

„NOWY WYMIAR STUDIOWANIA w WSPIA"

WND POWR.03.05.00-00-z045/17, działanie 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego.

Zgodnie z obowiązkiem wynikającym z art. 13 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 (RODO), poniżej przekazujemy informacje dotyczące przetwarzania Pani/Pana danych osobowych:

1. Administratorem Państwa danych osobowych jest Wyższa Szkołą Prawa i Administracji Rzeszowska Szkoła Wyższa z siedzibą w Rzeszowie, ul. Cegielniana 14, 35-310 Rzeszów; sekretariatr@wspia.eu, tel.: 17 8670400,
2. Administrator powołał Inspektora Ochrony Danych, z którym kontakt jest możliwy pod adresem email: Magdalena.Czech@wspia.eu.
3. Państwa dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem prowadzonym w trybie zapytania ofertowego Na zakup urządzeń, sprzętu i oprogramowania wraz z ich instalacją i wdrożeniem – jako wsparcie informatycznych narzędzi zarządzania WSPiA- w celu dostosowania jakości kształcenia w Uczelni obejmujących:

1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;

2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;

w ramach projektu pn.:

„NOWY WYMIAR STUDIOWANIA w WSPIA"

WND POWR.03.05.00-00-z045/17, działanie 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego.

4. Państwa dane osobowe mogą być udostępnione:
Instytucji Zarządzającej Programem Operacyjnym;
Podmiotom współpracującym z Zamawiającym w przypadku gdy będzie to niezbędne do prawidłowej realizacji zamówienia;
Podmiotom, które złożą żądanie wglądu do dokumentacji związanej z prowadzonym postępowaniem w związku z zapytaniem ofertowym – zgodnie z Wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 z dnia 22 sierpnia 2019 roku, 21 grudnia 2020 roku, MIiR/2014-2020/12(5) (WYTYCZNE);
Państwa dane osobowe mogą zostać udostępnione w związku z upublicznieniem wyników postępowania o zamówienie zgodnie z WYTYCZNYMI;
5. Państwa dane będą przechowywane do upływu terminu trwałości zrealizowanego projektu pn.: „Nowy wymiar studiowania w WSPiA", a następnie do czasu ich archiwizowania zgodnie z umową o dofinansowanie zawartą pomiędzy Zamawiającym, a Instytucją Zarządzającą Programem Operacyjnym.
6. Prawa osób, których dane dotyczą:
Posiadają Państwo:
1) prawo dostępu do swoich danych osobowych;
2) prawo do sprostowania Państwa danych osobowych z zastrzeżeniem, że skorzystanie z tego prawa nie może skutkować zmianą wyniku postępowania o udzielenie niniejszego zamówienia ani zmianą postanowień zawartej umowy oraz nie może naruszać integralności dokumentacji procedury udzielenia zamówienia w związku z Zapytaniem ofertowym;
3) prawo do wniesienia skargi do Prezes Urzędu Ochrony Danych Osobowych, gdy uznają Państwo, że przetwarzanie danych osobowych Państwa dotyczących narusza przepisy RODO;
4) prawo żądania od Administratora ograniczenia przetwarzania danych osobowych, z zastrzeżeniem przypadków o których mowa w art. 18 ust. 2 RODO;
Nie przysługuje Państwu:
1) w związku z art. 17 ust. 3 lit b, d lub e RODO prawo do usunięcia danych osobowych;
2) prawo do przenoszenia danych osobowych, o których mowa w art. 20 RODO;

3) na podstawie art. 21 RODO Prawo sprzeciwu, wobec przetwarzania danych osobowych, ponieważ podstawą prawną przetwarzania Państwa danych osobowych jest art. 6 ust 1 lit c RODO;

W przypadku nie wyrażenia zgody na przetwarzanie danych osobowych złożona oferta w tym postępowaniu zostanie odrzucona.

Oświadczenie *

☐ **Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie określonym w powyższej Klauzuli Informacyjnej.**

I.

☐ **Nie wyrażam zgody na przetwarzanie moich danych osobowych w zakresie określonym w powyższej Klauzuli Informacyjnej.**

II.

***zaznacz właściwe**

.....
(data i podpis osoby fizycznej)

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 8 do Warunków

DOKUMENT GWARANCYJNY
(wzór)

Nazwa Wykonawcy .....

Adres Wykonawcy .....

I Gwarancja jakości

1. Wykonawca oświadcza, że udziela gwarancji jakości na wymienione niżej urządzenia i sprzęt wchodzące w zakres przedmiotu Umowy wraz z ich instalacją i wdrożeniem tj.: wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
   a) .....
   b) .....
   c) .....

2. Okres gwarancji wynosi 36 miesięcy licząc od dnia .....
3. Wykonawca oświadcza, że dostarczone elementy przedmiotu Umowy opisane w pkt. 1 są zgodne z Umową i zostały prawidłowo zainstalowane co umożliwia korzystanie z tych przedmiotów zgodnie z ich przeznaczeniem, a w przypadku ujawnienia się ich wad w okresie gwarancji zobowiązuje się do:
   1) usunięcia wady na własny koszt
   2) lub do wymiany przedmiotu Umowy na przedmiot wolny od wad.

   w terminach określonych przez Zamawiającego.

4. Gwarancja nie wyłącza, nie ogranicza ani nie zawiesza uprawnień Zamawiającego wynikających z przepisów Kodeksu Cywilnego o rękojmi za wady rzeczy sprzedanej.

II Gwarancja obejmująca oprogramowania wchodzące w skład przedmiotu Umowy.

1. Wykonawca oświadcza, że dostarczył zgodnie z wszystkimi wymogami Umowy specjalistyczne oprogramowania do zabezpieczenia 232 komputerów podczas egzaminu – licencje bezterminowe; wraz z ich systematycznymi aktualizacjami w okresie 4 lat, licząc od daty wdrożenia tj. zgodnie ze Specyfikacją Nr 2, stanowiącą Załączniki nr 2 do tej Umowy.

2. Wykonawca oświadcza, że udziela gwarancji na przedmiot Umowy w zakresie określonym w pkt. 1 gwarancji, o której mowa w części II - **na okres 36 miesięcy** licząc od dnia ..... roku

3. W ramach gwarancji Wykonawca jest zobowiązany do usunięcia na swój koszt i ryzyko wszystkich wykrytych przez Zamawiającego wad tj.: awarii, błędów, usterek, przedmiotu Umowy.
4. Reagowania na zgłoszone awarie, błędy lub usterki utrudniające lub uniemożliwiające korzystanie z oprogramowań określonych w pkt. 1 gwarancji o której mowa w części II odbywają się w następującym trybie:
   1) w razie wystąpienia awarii, rozumianej jako nagłe i nieprzewidziane uszkodzenie programu/ów uniemożliwiające jego użycie – czas reakcji do 4 godziny robocze, czas naprawy do 20 godzin roboczych;
   2) w razie wystąpienia błędu w oprogramowaniu/ach, rozumianego jako brak poprawnego prawidłowego działania programu lub jego elementu/funkcji umożliwiającego jednak pracę przez zastosowanie tzw. obejścia - czas reakcji do 16 godzin roboczych, czas naprawy do 5 dni roboczych;
   3) w razie wystąpienia usterki, rozumianej jako „kosmetyczna" wada techniczna obniżająca jakość działania programu/ów - czas reakcji do16 godzin roboczych, czas naprawy 7 dni roboczych;

   gdzie:

   czas reakcji - to czas, jaki upłynie od przyjęcia zgłoszenia wady do potwierdzenia rozpoczęcia analizy zgłoszenia przez Wykonawcę;

   czas naprawy - to czas jaki upłynie od potwierdzenia przyjęcia zgłoszenia do jego całkowitego rozwiązania, przy czym do czasu naprawy zalicza się wyłącznie czas pracy Wykonawcy.
5. Niezależnie od udzielonej przez Wykonawcę Gwarancji, o której mowa w części II, Zamawiającemu przysługiwać będą roszczenia z tytułu wad prawnych przedmiotu Umowy określonego w pkt. 1 tej Gwarancji do których stosuje się odpowiednio przepisy Kodeksu cywilnego o rękojmi za wady prawne.

.....

(data i podpis uprawnionego przedstawiciela Wykonawcy)

nr zapytania ofertowego 8/KON/z045/2021

Załącznik nr 9 do Warunków

WZÓR UMOWY

Na zakup urządzeń, sprzętu i oprogramowania wraz z ich instalacją i wdrożeniem – jako wsparcie informatycznych narzędzi zarządzania WSPiA- w celu dostosowania jakości kształcenia w Uczelni obejmujących:

1) **wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;**
2) **specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;**

w ramach projektu pn.: „NOWY WYMIAR STUDIOWANIA w WSPIA" WND POWR.03.05.00-00-z045/17, działanie 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego – zwana dalej Umową,

zawarta w dniu ……. w Rzeszowie pomiędzy:

Wyższą Szkołą Prawa i Administracji Rzeszowską Szkołą Wyższą z siedzibą w Rzeszowie, ul Cegielniana 14, 35-310 Rzeszów, reprezentowaną przez:
Prof. dr hab. Jerzego Posłusznego - Rektora
zwaną w dalszej treści umowy **„Zamawiającym",**

a

…… z siedzibą w ..... ul. ....., wpisaną do ....., NIP ……., REGON ……..,
reprezentowaną przez
…….
zwanym w dalszej treści umowy **„Wykonawcą",**
Łącznie zwanymi w dalszej treści Umowy „Stronami".

Niniejsza Umowa została zawarta w wyniku rozstrzygnięcia zapytania ofertowego przeprowadzonego na podstawie Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 z dnia 21 grudnia 2020 roku, MIiR/2014-2020/12(5).

WYJAŚNIENIE POJĘĆ
§ 1

Użyte w niniejszej Umowie pojęcia oznaczają:

1. **Zamawiający -** WSPiA Rzeszowska Szkoła Wyższa z siedzibą w Rzeszowie.
2. **Wykonawca –** podmiot który realizuje Przedmiot Umowy.
3. **Projekt -** „Nowy wymiar studiowania w WSPiA" – WND POWR.03.05.00-00-z045/17 w ramach działania 3.5 Kompleksowe programy szkół wyższych, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020 współfinansowany ze środków Europejskiego Funduszu Społecznego.

4. **Warunki –** WARUNKI ZAMÓWIENIA NA ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI OBEJMUJĄCYCH:
   1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
   2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;
5. **Zapytanie –** Zapytanie ofertowe NR 8/KON/z045/2021 obejmujące Warunki zamówienia o których mowa w ust. 4;
6. **Wytyczne** - Wytyczne w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 z dnia 21 grudnia 2020 roku, MIiR/2014-2020/12(5)
7. **System nr 1** - wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
8. **System nr 2 -** specjalistyczne oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu – licencje bezterminowe, systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożenia;
9. **Specyfikacja nr 1 -** Specyfikacja Techniczna dotycząca **Systemu nr 1** - wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
10. **Specyfikacja nr 2 -** Specyfikacja Techniczna dotycząca **Systemu nr 2 -** specjalistyczne oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu – licencje bezterminowe; systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożenia;
11. **Zamówienie –** odpłatna Umowa określona w ust. 12 zawarta zgodnie z warunkami wynikającymi z umowy o dofinansowania projektu pomiędzy Zamawiającym, a Wykonawcą dotyczącej realizacji przedmiotu zapytania ofertowego.
12. **Umowa -** Umowa NA ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI OBEJMUJĄCYCH:
   1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej;
   2) specjalistyczne oprogramowanie do zabezpieczenia komputerów podczas egzaminu – licencje bezterminowe;
13. **IZPO** – Instytucja Zarządzająca Programem Operacyjnym.

PRZEDMIOT UMOWY
§ 2

1. Przedmiotem Umowy jest ZAKUP URZĄDZEŃ, SPRZĘTU I OPROGRAMOWANIA WRAZ Z ICH INSTALACJĄ I WDROŻENIEM - JAKO WSPARCIA INFORMATYCZNYCH NARZĘDZI ZARZĄDZANIA WSPIA - W CELU DOSTOSOWANIA JAKOŚCI KSZTAŁCENIA W UCZELNI OBEJMUJĄCYCH:
   1) wyposażenie sali egzaminacyjnej w infrastrukturę logiczną i niezbędne elementy do obsługi sieci komputerowej
   2) specjalistyczne oprogramowanie do zabezpieczenia 232 komputerów podczas egzaminu – licencje bezterminowe; systematyczna aktualizacja w okresie 4 lat, licząc od daty wdrożenia;
2. Przedmiot Umowy został szczegółowo określony odpowiednio:
   1) w **Specyfikacji nr 1** stanowiącej załącznik nr 1 do niniejszej Umowy;
   2) w **Specyfikacji nr 2** stanowiącej załącznik nr 2 do niniejszej Umowy.

TERMIN I MIEJSCE REALIZACJI PRZEDMIOTU UMOWY
§ 3

1. Wykonawca zobowiązany jest zrealizować w całości przedmiot Umowy do dnia ……
2. Końcowy termin realizacji przedmiotu Umowy określony w ust. 1 oznacza termin końcowego bezusterkowego odbioru przedmiotu Umowy.
3. Przedmiot umowy zrealizowany zostanie w siedzibie Zamawiającego - WSPiA Rzeszowskiej Szkole Wyższej, Cegielniana 14, 35-310 Rzeszów.

WSTĘPNE OŚWIADCZENIA I ZOBOWIĄZANIA STRON UMOWY
§ 4

1. Wykonawca oświadcza że:
   1) jest podmiotem oferującym wysokiej jakości dostawy i usługi związane z realizacją przedmiotu Umowy, posiadając wiedzę i odpowiednie kompetencje niezbędne do wykonania Systemu nr 1 i Systemu nr 2 oraz ich instalacji i wdrożenia zgodnie z postanowieniami Umowy;
   2) posiada uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
   3) posiada wiedzę oraz doświadczenie niezbędne do zrealizowania przedmiotu Umowy;
   4) posiada odpowiedni potencjał ekonomiczny i techniczny niezbędny do realizacji przedmiotu Umowy;
   5) dysponuje osobami zdolnymi do wykonania przedmiotu Umowy;
   6) jest świadomy, iż terminowe wykonanie przedmiotu Umowy ma kluczowe znaczenie dla Zamawiającego.
2. Wykonawca zobowiązuje się do wykonania przedmiotu Umowy:
   1) zgodnie ze złożoną ofertą, z treścią Umowy, interesem Zamawiającego, wszystkimi obowiązującymi przepisami prawa w Polsce i Unii Europejskiej, w sposób nienaruszający praw osób trzecich;
   2) z zachowaniem najwyższej profesjonalnej staranności z uwzględnieniem aktualnych, światowych standardów realizacji w tym w zakresie obsługi gwarancyjnej przedmiotu Umowy, zapewniając docelowe korzystanie przez Zamawiającego z rozwiązań przyjętych w Systemie nr 1 i Systemie nr 2 w szczególności:
      a) zabezpieczających integralność, poufność i bezpieczeństwo danych;
      b) przyjaznych dla użytkowników;
      c) gwarantujących ciągłe, stabilne funkcjonowanie elementów przedmiotu Umowy;

3. Zamawiający zobowiązuje się do współpracy z Wykonawcą przy realizacji przedmiotu Umowy. Jeżeli Strony nie uzgodniły na piśmie i nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji Umowy, jako obowiązku Zamawiającego, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca. Niniejsza klauzula modyfikuje postanowienia art. 640 Kodeksu cywilnego.

PROCEDURA ODBIORU PRZEDMIOTU UMOWY
§ 5

1. Odbiór przedmiotu Umowy nastąpi jednorazowo na podstawie bezusterkowego protokołu odbioru podpisanego przez uprawnionych przedstawicieli obu Stron Umowy.
2. Wykonawca zobowiązany jest zgłosić na piśmie Zamawiającemu gotowość do odbioru przedmiotu Umowy najpóźniej w terminie 30 dni przed terminem określonym w **§ 3 ust 1** Umowy.
3. Zamawiający niezwłocznie po zawiadomieniu przez Wykonawcę o gotowości do odbioru przedmiotu Umowy przystąpi do czynności odbioru.

4. Jeżeli w toku czynności odbiorowych stwierdzone zostaną wady, niezgodności z Umową lub inne nieprawidłowości, Zamawiający wyznaczy Wykonawcy odpowiedni termin do ich usunięcia.
5. Wykonawca po usunięciu wszystkich wad, usterek i nieprawidłowości, w terminie wyznaczonym przez Zamawiającego zgłosi ponownie gotowość do odbioru przedmiotu Umowy.
6. Jeżeli w toku czynności odbioru ponownie stwierdzone zostaną wady, niezgodności z Umową lub inne nieprawidłowości, Zamawiający odmówi podpisania protokołu odbioru przedmiotu Umowy. Będzie miał również prawo do naliczenia kar umownych i odstąpienia od Umowy w przypadkach opisanych w Umowie.
7. Bezusterkowy protokół odbioru stanowi podstawę do wystawienia faktury VAT.

LICENCJE NA OPROGRAMOWANIA
STANOWIĄCE ELEMENTY PRZEDMIOTU UMOWY
§ 6

1. Oprogramowania stanowiące elementy przedmiotu Umowy (**§ 2 ust. 1 pkt 2)**) są utworami w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (tekst jednolity Dz.U. 2018 poz. 1191 z późn. zm).
2. Wykonawca oświadcza, że jest uprawniony (należycie umocowany) do udzielania Zamawiającemu bezterminowych licencji na korzystanie z oprogramowań, o którym mowa w ust. 1, zgodnie z ich przeznaczeniem oraz do ich aktualizacji w okresie 4 lat licząc od daty wdrożenia oprogramowań.
3. Wykonawca gwarantuje, że oprogramowania, o których mowa w ust. 1 są wolne od wad prawnych i jednocześnie oświadcza, że w sytuacji gdy do realizacji przedmiotu Umowy niezbędne będzie korzystanie z oprogramowań innych podmiotów, jest on uprawniony, na podstawie odrębnych umów, do korzystania z takich oprogramowań na wszystkich polach eksploatacji niezbędnych do wykonania przedmiotu Umowy oraz korzystania przez Zamawiającego z wdrożonych oprogramowań przez czas nieokreślony.
4. Wykonawca ponosi pełną odpowiedzialność za wszelkie szkody, poniesione przez Zamawiającego w wyniku wystąpienia wad prawnych każdego z oprogramowań, o których mowa w ust. 1, w szczególności w przypadku wystąpienia przez osoby trzecie przeciwko Zamawiającemu z roszczeniem dotyczącym naruszenia ich praw własności intelektualnej w odniesieniu do chociażby jednego z tych oprogramowań. W takim wypadku Wykonawca zobowiązuje się niezwłocznie zwolnić Zamawiającego z obowiązku świadczenia na rzecz osób trzecich i naprawić wynikłą stąd szkodę.
5. W przypadku niemożności korzystania przez Zamawiającego z oprogramowań, o których mowa w ust. 1 w związku z roszczeniami opisanym w ust. 4, Wykonawca niezwłocznie, według swojego wyboru oraz na swój koszt:
   1) uzyska dla Zamawiającego licencję do dalszego korzystania z oprogramowań będącego przedmiotem sporu, lub
   2) wymieni oprogramowania na nowe, posiadające te same cechy i funkcjonalności jak dotychczasowe lub zmodyfikuje oprogramowanie/oprogramowania na niepowodujące naruszenia praw osób trzecich.
6. Wykonawca (Licencjodawca) oświadcza, że:
   1) udziela Zamawiającemu (Licencjobiorcy) bezterminowych licencji na każde z oprogramowań, o których mowa w ust. 1 zapewniając nieprzerwane i prawidłowe działanie urządzeń i sprzętów, których wszystkie funkcjonalności zostały szczegółowo opisane w Specyfikacjach.
   2) aktualizował będzie powyższe oprogramowania w okresie 4 lat licząc od daty ich wdrożenia.
7. W przypadku konieczności zapewnienia transmisji danych pomiędzy oprogramowaniami, a innym systemami informatycznymi, Wykonawca przekaże Zamawiającemu strukturę danych do przenoszenia danych do/z oprogramowań.
8. Wraz z instalacją oprogramowań, o której mowa w ust. 1, Wykonawca zainstaluje wersje elektroniczne dokumentacji użytkowej każdego z oprogramowań w języku polskim. Dostarczy

również aktualną wersję dokumentacji użytkowej w wersji elektronicznej w czasie trwania okresu gwarancyjnego.

WYNAGRODZENIE ZA WYKONANIE PRZEDMIOTU UMOWY
§ 7

1. Wynagrodzenie ryczałtowe z tytułu wykonania całego przedmiotu Umowy określonego w § 2 wynosi netto:…… złotych (słownie:……) plus podatek VAT tj. łącznie brutto ……złotych (słownie:……).
2. Dla uniknięcia wątpliwości interpretacyjnych Strony zgodnie potwierdzają, że kwota wynagrodzenia wskazana w ust. 1 stanowi wynagrodzenie ryczałtowe, obejmujące wszystkie koszty i wydatki Wykonawcy, stanowiące całość wynagrodzenia Wykonawcy w zakresie realizacji przedmiotu Umowy, w tym opłaty z tytułu udzielenia wszystkich bezterminowych licencji niewyłącznych, a ponadto, że w żadnym wypadku Zamawiający nie będzie ponosił odpowiedzialności za roszczenia przewyższające tę kwotę.
3. Powyższa kwota wyczerpuje wszelkie roszczenia Wykonawcy w stosunku do Zamawiającego związane z realizacją Umowy i Wykonawcy nie przysługuje podwyższenie wynagrodzenia, ani zwrot od Zamawiającego jakichkolwiek kosztów lub wydatków poniesionych przez Wykonawcę w związku z realizacją Umowy, nawet jeśli w czasie zawarcia Umowy nie można było przewidzieć rozmiaru lub kosztów wykonywanych prac.
4. Podstawą wystawienia przez Wykonawcę faktury VAT jest bezusterkowy protokół odbioru całego przedmiotu Umowy podpisany przez uprawnionych przedstawicieli obu Stron Umowy.
5. Zapłata wynagrodzenia dokonywana zostanie przelewem - w terminie do 30 dni od dnia dostarczenia Zamawiającemu prawidłowo wystawionej faktury VAT, zgodnie z treścią ust. 4 - na rachunek Wykonawcy wskazany na fakturze VAT**.**

POUFNOŚĆ ORAZ OCHRONA DANYCH OSOBOWYCH
§ 8

1. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji technicznych, organizacyjnych i handlowych, udostępnionych przez Zamawiającego w związku z wykonywaniem niniejszej Umowy i do niewykorzystywania ich w jakimkolwiek innym celu niż do wykonania niniejszej Umowy, a także do zachowania w tajemnicy informacji, których ujawnienie osobom trzecim lub wykorzystanie przez Wykonawcę mogłoby narazić interes Zamawiającego.
2. Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich danych dotyczących działalności Zamawiającego oraz danych przetwarzanych w systemach informatycznych Zamawiającego, a także informacji powziętych w związku z przygotowaniem oferty i realizacją niniejszej Umowy, obejmujących koncepcję, rozwiązania merytoryczne, formalne i organizacyjne w zakresie realizowanych Systemów.
3. Wykonawca zobowiązuje się do zachowania wszelkich informacji związanych z przetwarzanymi danymi osobowymi w systemach informatycznych Zamawiającego, a w szczególności do nie kopiowania, drukowania i udostępniania tych danych. Wykonanie kopii przez Wykonawcę dopuszczalne jest wyłącznie w uzasadnionych przypadkach, każdorazowo po uzgodnieniu z Zamawiającym i odnotowaniu w stosownym protokole podpisanym przez pełnomocników ze strony Wykonawcy oraz Zamawiającego;
4. Obowiązek zachowania tajemnicy nie dotyczy informacji powszechnie znanych lub co, do których Wykonawca uzyskała pisemną zgodę od Zamawiającego na ich ujawnienie;

ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY
§ 9

1. Wykonawca, najpóźniej do 3 dni roboczych od daty zawarcia Umowy, wnosi zabezpieczenie należytego wykonania Umowy w wysokości …….. **zł brutto**, to jest 10% ceny całkowitej (brutto) podanej w ofercie, (słownie: ……złotych brutto), w formie ……..
2. Treść gwarancji zabezpieczającej należyte wykonanie Umowy powinna być zgodna z wymogami określonymi w Warunkach zwartych w Zapytaniu ofertowym, stanowiącym **Załącznik nr 4** do niniejszej Umowy.
3. Część zabezpieczenia w wysokości 70 % kwoty wymienionej w ust. 1 zostanie zwrócona Wykonawcy w terminie 30 dni od dnia wykonania przedmiotu Umowy tj. podpisania bezusterkowego protokołu odbioru przez uprawnionych przedstawicieli obu Stron Umowy.
4. Pozostałe 30% kwoty zabezpieczenia zostanie zwrócone Wykonawcy w ciągu 30 dni po upływie 36-miesięcznego okresu gwarancji i rękojmi oraz wypełnieniu wszystkich zobowiązań wynikających z gwarancji i rękojmi w tym okresie.
5. W sytuacji, gdy wystąpi konieczność przedłużenia terminu realizacji niniejszej Umowy w przypadkach o których mowa w § 14, Wykonawca przed podpisaniem aneksu lub najpóźniej w dniu jego podpisywania, zobowiązany jest do przedłużenia terminu ważności wniesionego zabezpieczenia należytego wykonania Umowy, albo jeśli nie jest to możliwe, do wniesienia nowego zabezpieczenia na okres wynikający z aneksu do Umowy.
6. Wartość zabezpieczenia należytego wykonania Umowy, o którym mowa w ust. 1 służy do pokrycia wszelkich roszczeń z tytułu gwarancji, rękojmi, roszczeń z tytułu wad prawnych oprogramowań stanowiących elementy przedmiotu Umowy, roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, zapłaty kar umownych i odszkodowania uzupełniającego.

GWARANCJE
§ 10

1. Wykonawca udziela Zamawiającemu gwarancji jakości na urządzenia i sprzęty wchodzące w zakres przedmiotu Umowy wraz z ich instalacją i wdrożeniem na okres 36 miesięcy - licząc od dnia dokonania bezusterkowego odbioru przedmiotu Umowy – zgodnie z dokumentem gwarancyjnym stanowiącym **Załącznik nr 5** do Umowy.
2. Gwarancja, o której mowa w ust. 1 obejmuje oświadczenie Wykonawcy, że elementy przedmiotu Umowy określone w ust. 1 spełniają wymogi jakościowe i techniczne oraz zostały wykonane zgodnie z Umową.
3. Gwarancja jakości obejmuje zarówno wady niewykryte w momencie odbioru przedmiotu Umowy, jak też wszelkie nieprawidłowości i wady fizyczne powstałe z przyczyn występujących po stronie Wykonawcy.
4. Zgłoszenie Zamawiającego dotyczące wad przedmiotu Umowy, na który została udzielona gwarancja jakości następuje telefonicznie (nr tel.) lub pocztą elektroniczną pod adres e-mail …. .. . w godzinach od 7:30 do 15:30, w dni robocze (od poniedziałku do piątku z wyłączeniem dni wolnych od pracy). Zgłoszenia dokonane po godz. 15:30 traktowane są jako zgłoszone w dniu następnym.
5. Wykonawca zobowiązuje się w ramach udzielonej gwarancji jakości do usunięcia wad fizycznych elementów przedmiotu Umowy określonych w ust. 1 lub dostarczenia rzeczy wolnej od wad, w terminie określonym przez Zamawiającego.
6. Udzielona gwarancja jakości nie wyłącza, nie ogranicza, ani nie zawiesza uprawnień Zamawiającego wynikających z przepisów o rękojmi za wady rzeczy sprzedanych zawartych w Kodeksie cywilnym.
7. Odpowiedzialność Wykonawcy z tytułu rękojmi za wady fizyczne elementów przedmiotu Umowy określonych w ust. 1 wynosi 36 miesięcy, licząc od daty odbioru przedmiotu Umowy.

8. Wykonawca oświadcza też, że udziela Zamawiającemu gwarancji na prawidłowe działanie dostarczonych i zainstalowanych oprogramowań wchodzących w skład przedmiotu Umowy, na okres 36 miesięcy licząc od dnia dokonania bezusterkowego odbioru przedmiotu Umowy – zgodnie z dokumentem gwarancyjnym stanowiącym **Załącznik nr 5** do Umowy.
9. Gwarancja na oprogramowania obejmuje zarówno wady niewykryte w momencie odbioru Przedmiotu Umowy jak też wszelkie nieprawidłowości w działaniu oprogramowań powstałe z przyczyn występujących po stronie Wykonawcy.
10. Zgłoszenia Zamawiającego dotyczące wad lub nieprawidłowości w działaniu oprogramowań będą przekazywane Wykonawcy telefonicznie (nr tel.) lub pocztą elektroniczną pod adres e-mail .... w godzinach od 7:30 do 15:30, w dni robocze (od poniedziałku do piątku z wyłączeniem dni wolnych od pracy). Zgłoszenia dokonane po godz. 15:30 traktowane są jako zgłoszone w dniu następnym.
11. Po otrzymaniu zgłoszenia, Wykonawca zobowiązuje się do usunięcia wykrytej(-ych) wad lub nieprawidłowości oprogramowania własnym staraniem i na swój wyłączny koszt.
12. W przypadku braku możliwości zapewnienia pełnego korzystania z oprogramowania, Wykonawca zobowiązuje się do przywrócenia pełnej funkcjonalności tego oprogramowania, w niżej określonych terminach, uzależnionych od wagi poszczególnych dostępności:

1) w razie wystąpienia awarii, rozumianej jako nagłe i nieprzewidziane uszkodzenie programu/ów uniemożliwiające jego użycie – usunięcie awarii nastąpi w terminie 1 dnia roboczego;
2) w razie wystąpienia błędu w oprogramowaniu/ach, rozumianego jako brak poprawnego prawidłowego działania programu lub jego elementu/funkcji umożliwiającego jednak pracę przez zastosowanie tzw. obejścia – usunięcie błędu nastąpi w terminie do 5 dni roboczych;
3) w razie wystąpienia usterki, rozumianej jako „kosmetyczna" wada techniczna obniżająca jakość działania programu/ów - usunięcie usterki nastąpi w terminie do 7 dni roboczych;

gdzie:

za dzień roboczy Strony uznają każdy dzień roku niebędący dniem wolnym od pracy w rozumieniu przepisów prawa. Przyjmuje się, że sobota jest dniem wolnym dla Zamawiającego."

13. Niezależnie od udzielonych przez Wykonawcę gwarancji, o których mowa w ust. 8 Zamawiającemu przysługiwać będą roszczenia z tytułu wad prawnych oprogramowań, do których stosuje się odpowiednio przepisy Kodeksu cywilnego o rękojmi za wady prawne oraz zawartą Umowę.
14. Wykonawca jest zobowiązany usunąć na własny koszt wady prawne oprogramowań, ponosząc pełną odpowiedzialność za wszelkie szkody z tego tytułu zgodnie z postanowieniami niniejszej Umowy.

ODSZKODOWANIE I KARY UMOWNE
§ 11

1. Wykonawca ponosi odpowiedzialność za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem Umowy.
2. Zamawiający ma prawo naliczenia kary umownej za każdy dzień opóźnienia Wykonawcy w wykonaniu przedmiotu Umowy w wysokości 0,1% wynagrodzenia brutto określonego w § 7 ust 1.
3. Zamawiający ma prawo do naliczenia kary umownej w trakcie obowiązywania Umowy i okresu gwarancyjnego, za każdy dzień opóźnienia w usunięciu wad elementów przedmiotu Umowy określonych w § 10 ust. 1 Umowy oraz awarii, błędów, usterek w funkcjonowaniu oprogramowań wchodzących w skład przedmiotu Umowy – w wysokości 0,1 % wynagrodzenia brutto określonego w § 7 ust 1.

4. Za odstąpienie od Umowy przez którąkolwiek ze Stron Umowy z przyczyn występujących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia ryczałtowego brutto wskazanego w § 7 ust. 1.
5. Naliczenie kary umownej z jednego tytułu nie wyklucza możliwości naliczania kar umownych z innych tytułów.
6. Uiszczenie przez Wykonawcę jakichkolwiek kar umownych wynikających z niniejszej Umowy nie uchybia uprawnieniu Zamawiającego do dochodzenia na zasadach ogólnych, odszkodowania w wysokości przewyższającej wysokość zastrzeżonych kar umownych, do pełnej wysokości poniesionej szkody.
7. Kary umowne, o których mowa w niniejszej Umowie, płatne są w terminie 14 dni od dnia doręczenia do Wykonawcy żądania zapłaty.
8. Zamawiający może potrącać kary umowne określone w niniejszej Umowie z wynagrodzenia należnego Wykonawcy zgodnie z Umową.
9. Niezależnie od innych postanowień niniejszej Umowy oraz przepisów prawa, w przypadku powstania odpowiedzialności Zamawiającego wobec osób trzecich lub organów administracji publicznej wskutek niewykonania lub nienależytego wykonania niniejszej Umowy przez Wykonawcę, powstałych z przyczyn występujących po stronie Wykonawcy, Wykonawca niezwłocznie, w terminie określonym lub wynikającym z przepisów prawa, nie później jednak niż w terminie 7 (siedem) dni od zgłoszenia żądania w tym zakresie przez Zamawiającego, zwolni Zamawiającego z obowiązku świadczenia i pokryje wszelkie odsetki, kary oraz inne zobowiązania Zamawiającego wobec osób trzecich lub organów administracji publicznej wynikające z niewykonania lub nienależytego wykonania zobowiązań umownych przez Wykonawcę.

SIŁA WYŻSZA
§ 12

1. Przyjmuje się, że Siła Wyższa stanowi zdarzenie zewnętrzne, cechujące się: niemożliwością jego przewidzenia (należy ją rozumieć w ten sposób, iż przy obiektywnej ocenie zdarzeń ustalono najwyżej bardzo niski stopień prawdopodobieństwa jego pojawienia się) oraz niemożliwością zapobieżenia jego skutkom. Siła wyższa musi być zdarzeniem o nadzwyczajnych rozmiarach lub zasięgu lub nawet innym zdarzeniem jeżeli wymyka się ono spod ludzkiej kontroli.
2. Żadna ze Stron nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy, jeżeli zostało ono spowodowane działaniem Siły Wyższej.
3. W przypadku zaistnienia Siły Wyższej, Strona, której to zdarzenie dotyczy, bezzwłocznie poinformuje drugą Stronę na piśmie o zaistnieniu takiego zdarzenia oraz o jego wpływie na realizację zobowiązań wynikających z Umowy. Jeżeli Strony nie postanowią inaczej, Strony będą kontynuowały wykonywanie Umowy w zakresie, w jakim jest to możliwe pomimo występowania Siły Wyższej.
4. Wystąpienie zdarzenia o charakterze Siły Wyższej nie uwalnia od skutków niewykonania lub nienależytego wykonania obowiązków, które powinny być wykonane przed wystąpieniem lub po ustąpieniu tego zdarzenia. Strona dotknięta zdarzeniem o charakterze Siły Wyższej, zobowiązana jest do niezwłocznego podjęcia działań zmierzających do usunięcia skutków zdarzenia, w zakresie umożliwiającym jej prawidłowe wykonywanie obowiązków wynikających z Umowy.

ODSTĄPIENIE OD UMOWY
§ 13

1. Zamawiający ma prawo do odstąpienia od Umowy:
   1) jeżeli Wykonawca opóźnia się w realizacji przedmiotu Umowy, Zamawiający może wyznaczyć Wykonawcy odpowiedni dodatkowy termin do wykonania zobowiązania z zastrzeżeniem, że w razie bezskutecznego upływu wyznaczonego terminu odstąpi od Umowy. W celu uniknięcia wątpliwości interpretacyjnych Strony zgodnie potwierdzają, że za termin odpowiedni

w rozumieniu postanowienia niniejszego ustępu rozumieją termin nie krótszy niż 10 (dziesięć) dni roboczych. Wyznaczenie dodatkowego terminu nie zwalnia Wykonawcy z obowiązku zapłacenia kar umownych,

2) jeżeli Wykonawca nie przystąpił do realizacji Umowy, przerwał jej wykonywanie i mimo wezwania, nie kontynuuje jej realizacji,
3) w przypadku niewniesienia zabezpieczenia należytego wykonania Umowy w terminie lub w przypadku gdy treść gwarancji bankowej lub ubezpieczeniowej nie odpowiada wymaganiom określonym w Umowie;
4) w przypadku zajęcia majątku Wykonawcy przez uprawniony organ w celu zabezpieczenia lub egzekucji, jakiegokolwiek rozporządzenia majątkiem przez Wykonawcę, które może utrudnić lub uniemożliwić ewentualne zaspokojenie wierzyciela;
5) w przypadku przystąpienia przez Wykonawcę do likwidacji;
6) w przypadkach, gdy wystąpiła istotna zmiana okoliczności powodująca, że wykonanie przedmiotu Umowy nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć, bądź Zamawiającemu cofnięto, wstrzymano lub ograniczono dofinansowanie ze środków publicznych na realizację przedmiotu Umowy. W przypadku takiego odstąpienia, nie stosuje się kar określonych w niniejszej Umowie. Stronom nie przysługuje uprawnienie do dochodzenia odszkodowania.

2 Odstąpienie od Umowy następuje poprzez pisemne oświadczenie jednej ze Stron. Prawo odstąpienia od Umowy możne zostać zrealizowane w terminie 30 dni od dnia zajścia zdarzenia uzasadniającego odstąpienie od Umowy. Odstąpienie od Umowy poprzez pisemne oświadczenie danej Strony musi być poprzedzone wcześniejszym pisemnym poinformowaniem drugiej Strony o zamiarze odstąpienia z podaniem wszystkich jego przyczyn oraz z wyznaczeniem terminu do 7-dni na usuniecie tych przyczyn.

INNE ISTOTNE DLA STRON POSTANOWIENIA UMOWY
§ 14

1. Zmiana warunków Umowy zawartej w wyniku przeprowadzonego postępowania o zamówienia może nastąpić jeżeli zachodzi **jedna z następujących okoliczności:**

1.1. zmiany Umowy, niezależnie od ich wartości, nie są istotne, z zastrzeżeniem ust 3.
Zmianę postanowień zawartej Umowy **uznaje się za istotną** jeżeli:
1) zmienia ona ogólny charakter umowy w stosunku do charakteru w pierwotnym brzmieniu;
2) nie zmienia ogólnego charakteru umowy i zachodzi co najmniej jedna z następujących okoliczności:
a) zmiana wprowadza warunki, które, gdyby były postawione w postępowaniu prowadzonym w związku z niniejszym zapytaniem, to w tym postępowaniu wzięliby lub mogliby wziąć udział inni wykonawcy lub przyjęto by oferty innej treści,
b) zmiana narusza równowagę ekonomiczną umowy na korzyść Wykonawcy w sposób nieprzewidziany pierwotnie w Umowie,
c) zmiana znacznie rozszerza lub zmniejsza zakres świadczeń i zobowiązań wynikający z Umowy;
d) polega na zastąpieniu Wykonawcy, któremu Zamawiający udzielił zamówienia, nowym Wykonawcą, w innych przypadkach niż wymienione w pkt 2),

1.2. Wykonawcę, z którym Zamawiający zawarł Umowę w wyniku niniejszego postępowania ma zastąpić inny Wykonawca w wyniku połączenia, podziału, przekształcenia, upadłości, restrukturyzacji lub nabycia dotychczasowego Wykonawcy lub jego przedsiębiorstwa, o ile nowy Wykonawca spełnia warunki udziału w postępowaniu, nie zachodzą wobec niego przesłanki wykluczenia oraz nie powoduje to zmiany innych istotnych postanowień Umowy;

1.3. zostały spełnione łącznie następujące warunki, jeżeli nie prowadzą do zmiany charakteru Umowy:

1) konieczność zmiany spowodowana została okolicznościami, których Zamawiający, pomimo zachowania należytej staranności nie mógł przewidzieć;
2) wartość zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w Umowie.

2. Nie jest istotną zmianą umowy przedłużenie terminu realizacji przedmiotu zamówienia o okres nie dłuższy niż 30 dni.
3. **Zmiana istotnych warunków Umowy może nastąpić jeżeli:**
   1) wystąpiło działanie Siły Wyższej, o której mowa w § 12;
   2) wystąpiły zmiany powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy;
   3) nastąpiła uzasadniona konieczność zmiany warunków płatności; w szczególności wynikająca z braku terminowego otrzymania środków finansowych na realizację Umowy;

4 Możliwość przesunięcia terminu realizacji Umowy powyżej 30 dni uzależniona jest od uprzedniej zgody organu NCBR oraz od zaistnienia i udokumentowania okoliczności przemawiających za zmianą terminu, z korzyścią dla realizacji przedmiotu Umowy, na rzecz Zamawiającego.

5 Strony ustalają, że postanowienia niniejszej Umowy powinny być interpretowane łącznie z wymienionymi dalej Załącznikami stanowiącymi integralną część niniejszej Umowy. Jakiekolwiek wyrażenia użyte w Załącznikach mają znaczenie nadane im w Umowie, chyba, że z treści Załącznika wynika wyraźnie inne znaczenie.

6 Bez uzyskania uprzedniej pisemnej zgody Zamawiającego, Wykonawca nie może przenieść jakichkolwiek wierzytelności, wynikających z Umowy na inny podmiot.

7 Wszelkie zmiany, uzupełnienia i oświadczenia dotyczące niniejszej Umowy wymagają zgody Stron wyrażonej pisemnie pod rygorem nieważności.

8 Wszelkie oświadczenia Stron uważać się będzie za skuteczne, jeśli zostaną skierowane w formie pisemnej na poniższe adresy lub e-mailem pod warunkiem uzyskania potwierdzenia od drugiej strony:

1) dla Wykonawcy:
   ……
   ……
   ……
   e-mail: …….

2) dla Zamawiającego:
   Marek Rogalski
   Wyższa Szkoła Prawa i Administracji
   Rzeszowska Szkoła Wyższa z siedzibą w Rzeszowie
   ul. Cegielniana 14
   35-310 Rzeszów
   e-mail: marek.rogalski@wspia.eu

9 W sprawach nieuregulowanych w niniejszej Umowie zastosowanie będą miały odpowiednie przepisy ustawy Kodeks Cywilny, ustawy o prawie autorskimi i prawach pokrewnych oraz innych właściwych unormowań prawa polskiego.

10 W przypadku spraw spornych między Stronami, jakie mogą wyniknąć na tle realizacji niniejszej Umowy, Strony podejmą próbę mediacji lub innego pozasądowego sposobu rozwiązania sporu. W przypadku nieosiągnięcia porozumienia każda ze Stron może poddać sprawy sporne pod rozstrzygnięcie sądu właściwego miejscowo ze względu na siedzibę Zamawiającego.

11 Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, w tym jeden dla Zamawiającego i jeden dla Wykonawcy.

12 Integralną część Umowy stanowią następujące załączniki:

1) Specyfikacja Techniczna nr 1,
2) Specyfikacja Techniczna nr 2,
3) Oferta Wykonawcy;
4) Zapytanie ofertowe nr 8/KON/z045/2021,
5) Dokument gwarancyjny.