Polskie Radio – Regionalna Rozgłośnia w Białymstoku
„Radio Białystok" S.A.
ul. Świerkowa 1
15-328 Białystok

NIP: 542-00-03-367
REGON:050252837
Tel. (85) 7 456 200
Fax. (085) 7 443 423
Strona internetowa: www.radio.bialystok.pl
e-mail: sekretariat@radio.bialystok.pl

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA NA DOSTAWĘ SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA.

CPV: 48780000-9; 48223000-7; 32424000-1; 32420000-3; 80000000-4

Znak sprawy: ZP.215.04.2021

Podstawa prawna: **ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych – tekst jednolity (Dz. U. z 2021 r. poz. 1129), zwana dalej ustawą lub pzp.**

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie **podstawowym bez negocjacji** o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy, na podstawie art. 275 pzp oraz przepisów wykonawczych.

Szacunkowa wartość zamówienia nie przekracza kwoty, o której mowa w art. 3 pzp.

Ogłoszenie o zamówieniu zostało:
- zamieszczone w Biuletynie Zamówień Publicznych
- zarejestrowane na portalu https://ezamowienia.gov.pl/
- zamieszczone na stronie prowadzonego postępowania https://miniportal.uzp.gov.pl
- zamieszczone na stronie internetowej Zamawiającego https://www.radio.bialystok.pl/bip/

Termin składania ofert 09.12.2021 r. godz.10:00
Termin otwarcia ofert 09.12.2021 r. godz. 10:15

Zatwierdzam:

Wojciech Straszyński

Prezes Zarządu

I. ZAMAWIAJĄCY:

Polskie Radio – Regionalna Rozgłośnia w Białymstoku „RADIO BIAŁYSTOK" Spółka Akcyjna
Siedziba: Białystok
Adres Spółki : 15-328 Białystok, ul. Świerkowa 1,
Tel. (085) 7 456 200
Fax. (085) 7 443 423
Strona internetowa: www.radio.bialystok.pl
e-mail: sekretariat@radio.bialystok.pl
NIP: 542-00-03-367
REGON:050252837
KRS: 0000037873 Sąd Rejonowy w Białymstoku XII Wydział Gospodarczy KRS,
Kapitał zakładowy: 783 300 zł opłacony w całości
Znak sprawy: ZP.215.04.2021 (należy używać do oznaczania korespondencji kierowanej do Zamawiającego)

II. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym bez negocjacji, na podstawie art. 275 ustawy pzp oraz przepisów wykonawczych wydanych na jej podstawie.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa na rzecz Zamawiającego sprzętu komputerowego i oprogramowania zgodnie z Załącznikiem nr 1 do SWZ.

IV. OFERTY CZĘŚCIOWE

Zamawiający dopuszcza możliwość składania ofert częściowych na jedno lub więcej zadań objętych przedmiotem zamówienia:

Część 1 – Dostawa urządzeń typu UTM

Część 2 – Dostawa oprogramowania Exchange 2019

Opis techniczny przedmiotu zamówienia w ramach poszczególnych części zawiera Załącznik nr 1 do SWZ.

V. OFERTY WARIANTOWE

Zamawiający nie dopuszcza składania ofert wariantowych.

VI. ZAMÓWIENIA UZUPEŁNIAJĄCE

Zamawiający nie przewiduje udzielania zamówień uzupełniających.

VII. TERMIN WYKONANIA PRZEDMIOTU ZAMÓWIENIA

Zamawiający wymaga aby dostawa, wdrożenie i uruchomienie przedmiotu zamówienia nastąpiło do 28.02.2022 r.

VIII. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCEN SPEŁNIENIA TYCH WARUNKÓW

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

1.1. nie podlegają wykluczeniu z postępowania na podstawie art. 108 i art. 109 ust. 1 pkt 4, 5, 7 ustawy pzp;

1.2. spełniają warunki udziału w postępowaniu określone w art. 112 ust. 2 ustawy pzp:

a) zdolności do występowania w obrocie gospodarczym – Zamawiający nie określa warunku w tym zakresie
b) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie określa warunku w tym zakresie
c) sytuacji ekonomicznej lub finansowej – Zamawiający nie określa warunku w tym zakresie
d) zdolności technicznej lub zawodowej – Zamawiający nie określa warunku w tym zakresie

1.3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający wymaga, aby warunki określone w ust. 1 spełniał każdy z Wykonawców oddzielnie.

1.4. W przypadku wspólnego ubiegania się wykonawców o udzielenie zamówienia Zamawiający bada, czy nie zachodzą podstawy wykluczenia wobec każdego z tych wykonawców.

1.5. Oceniając zdolność techniczną lub zawodową, zamawiający może, na każdym etapie postępowania, uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.

2. Zasady udziału w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia:

2.1. Wykonawcy ubiegający się wspólnie o udzielenie zamówienia zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarciu umowy w sprawie zamówienia publicznego. Pisemne pełnomocnictwo winno być załączone do oferty.

2.2. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ponoszą solidarną odpowiedzialność za wykonanie zamówienia.

2.3. Zamawiający zastrzega sobie prawo żądania od Wykonawców składających ofertę wspólną, aby przed zawarciem umowy złożyli Zamawiającemu umowę określającą wzajemne ich relacje.

2.4. Przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający rozumie również Wykonawców będących wspólnikami spółki cywilnej.

2.5. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających brak podstaw wykluczenia jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne /t. j. Dz. U. z 2019 r. poz. 700 ze zm./. W tym celu Wykonawca zobowiązany jest do wskazania w złożonej ofercie jednoznacznie i wyczerpująco źródła (adresu) bazy danych lub postępowania, w którym u Zamawiającego znajdują się odpowiednie oświadczenia lub dokumenty.

2.6. Jeżeli wykonawca nie złoży oświadczeń i dokumentów, o których mowa w pkt. IX niniejszej SWZ, oświadczenia lub dokumenty są niekompletne, zawierają błędy, Zamawiający wezwie do ich złożenia, uzupełnienia, poprawienia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlegałaby odrzuceniu bez względu na ich złożenie, uzupełnienie czy poprawienie albo zajdą przesłanki unieważnienie postępowania.

3. Podwykonawcy:

3.1. Zamawiający dopuszcza udział podwykonawców.

3.2. Wykonawca jest zobowiązany do podania, jaka część zamówienia będzie realizowana przez podwykonawców oraz do podania nazw firm podwykonawców, o ile są mu wiadome.

3.3. Zamawiający wymaga, aby wobec podwykonawcy niebędącego podmiotem udostępniającym zasoby, nie zachodziły podstawy wykluczenia z postępowania na podstawie art. 108 i art. 109 ust. 1 pkt 4, 5, 7 ustawy pzp.

3.4. Powierzenie wykonania części zamówienia Podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia. Wykonawca będzie odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i ich pracowników w takim samym stopniu jakby to były działania, uchybienia i zaniedbania jego własnych pracowników.

IX. Wykaz oświadczeń lub dokumentów potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia

1. W celu wykazania braku podstaw do wykluczenia na podstawie art. 108 i 109 ust. 1 pkt 4, 5, 7 ustawy, wykonawcy wraz z ofertą zobowiązani są przedłożyć aktualne na dzień składania ofert oświadczenie o spełnieniu warunków udziału w postępowaniu oraz o braku podstaw do wykluczenia z postępowania, zgodnie z załącznikiem nr 3a do SWZ. Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
2. W przypadku składania oferty wspólnej, wykonawcy zobowiązani są wskazać pełnomocnika stosownie do postanowień art. 58, ust. 1 ustawy, a ponadto każdy z nich powinien załączyć oświadczenie, o którym mowa w pkt. IX ust. 1.
3. W przypadku, gdy ofertę w imieniu wykonawcy podpisuje pełnomocnik, wymaga się załączenia do oferty pełnomocnictwa określającego jego zakres i podpisanego przez osoby uprawnione do reprezentacji wykonawcy.
4. Zamawiający przed udzieleniem zamówienia wezwie wykonawcę, którego oferta została najwyżej oceniona do złożenia w terminie nie krótszym niż 5 dni, aktualnych na dzień złożenia następujących podmiotowych środków dowodowych:
   4.1 oświadczenia wykonawcy, w zakresie określonym w art. 108 ust. 1 pkt 5 ustawy o braku przynależności z innym wykonawcą, który złożył ofertę w niniejszym postępowaniu do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz.U. z 2021 r. poz. 275), a w przypadku zaistnienia ww. okoliczności – oświadczenia o przynależności z innym wykonawcą, który złożył ofertę w niniejszym postępowaniu do tej samej grupy kapitałowej i dokumentów lub informacji potwierdzających przygotowanie oferty niezależnie od ww. innego wykonawcy. Wzór oświadczeń zawiera załącznik nr 3b do SWZ; Wykonawcy wraz ze złożeniem przedmiotowego oświadczenia, mogą przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłóceń konkurencyjności w niniejszym postępowaniu o udzielenie zamówienia.
   4.2 Dokumenty podmiotów zagranicznych:
      - dokument potwierdzający, że nie otwarto likwidacji Wykonawcy,
      - informacja z odpowiedniego rejestru lub inny równoważny dokument.
5. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, ma zastosowanie § 7 Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. (Dz. U. 2020 poz. 2415) w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.
6. Jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, zamawiający może w każdym czasie wezwać wykonawcę lub

wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.

7. Zamawiający wzywa wykonawców, którzy w określonym terminie nie złożyli wymaganych przez zamawiającego oświadczeń lub dokumentów, o których mowa w art. 125 pzp lub są one niekompletne lub zawierają błędy. Zamawiający wzywa wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie.
8. Wykonawca, który korzysta z usług podwykonawców, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia – w zakresie, w jakim korzysta z podwykonawstwa – warunków udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w pkt. IX ust. 1 SWZ.

X. PRZEDMIOTOWE ŚRODKI DOWODOWE

1. Na potwierdzenie, że oferowana dostawa spełnia wymagania określone przez Zamawiającego w stosunku do przedmiotu zamówienia, Zamawiający żąda złożenia wraz z Ofertą:
   a) Specyfikacji technicznej zaoferowanego przedmiotu zamówienia jako przedmiotowego środka dowodowego, zgodnie z załącznikiem nr 1 do SWZ
2. Na żądanie Zamawiającego Wykonawca udostępni Karty katalogowe dostarczanych urządzeń z których wynikało będzie spełnienie wymogów technicznych (dopuszcza materiały w języku angielskim).

XI. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami, w szczególności składanie oświadczeń, wniosków, zawiadomień oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem dedykowanego formularza „Formularz do komunikacji" dostępnego na ePUAP, pod adresem: https://epuap.gov.pl/wps/portal oraz udostępnionego przez miniPortal, który dostępny jest pod adresem: https://miniportal.uzp.gov.pl/. We wszelkiej korespondencji związanej z przedmiotowym postępowaniem Zamawiający i Wykonawcy posługują się numerem postępowania wskazanym w SWZ. Dokumenty elektroniczne, składane są przez Wykonawcę za pośrednictwem „Formularza do komunikacji" jako załączniki.

2. Zamawiający może również kontaktować się z Wykonawcami za pomocą poczty elektronicznej (e-mail przetargi@radio.bialystok.pl) z zastrzeżeniem, że dokumenty lub oświadczenia, o których mowa w rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia wymienione w SWZ należy złożyć w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem

3. Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:
   - Jarosław Dobrowolski – tel. 0857456218, email: jdobrowolski@radio.bialystok.pl

4. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do następujących formularzy: „Formularz do złożenia, zmiany, wycofania oferty lub wniosku" oraz do „Formularza do komunikacji".

5. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z systemu miniPortal oraz Warunkach korzystania z elektronicznej platformy usług administracji publicznej (ePUAP).

6. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy: „Formularz złożenia, zmiany, wycofania oferty lub wniosku" i „Formularza do komunikacji" wynosi 150 MB.

7. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.

8. Sposób sporządzenia dokumentów elektronicznych musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 poz. 2452) oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 poz. 2415).

9. Ofertę, oświadczenia oraz środki dowodowe przekazuje się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem osobistym lub podpisem zaufanym.

XII. WADIUM

Zamawiający nie wymaga wniesienia wadium.

XIII. TERMIN ZWIĄZANIA OFERTĄ

Okres związania ofertą wynosi 30 dni i upływa 06.01.2022 r. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

XIV. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ TREŚCI SWZ

1. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem postępowania wskazanym w SWZ.

2. Wykonawca może zwrócić się do Zamawiającego z pisemną prośbą o wyjaśnienie treści SWZ.

3. Zamawiający odpowie Wykonawcom niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynie do Zamawiającego, nie później niż na 4 dni przed upływem terminu składania ofert. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępni na stronie internetowej prowadzonego postępowania. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynie po upływie terminu, o którym mowa powyżej, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpatrzenia.

4. W przypadku rozbieżności pomiędzy treścią niniejszej SWZ, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

5. Zamawiający nie przewiduje zwołania zebrania wszystkich Wykonawców w celu wyjaśnienia treści SWZ.

6. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść specyfikacji warunków zamówienia. Dokonaną zmianę treści specyfikacji zamawiający zamieszcza na stronie internetowej prowadzonego postępowania.

7. Zamawiający przedłuży termin składania ofert, jeżeli zmiany treści SWZ są istotne dla sporządzenia oferty lub wymagają od Wykonawców dodatkowego czasu na zapoznanie się ze zmianą SWZ i przygotowanie ofert oraz zamieści taką informację na stronie prowadzonego postępowania.

8. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku z zapytaniem do SWZ, o którym mowa w pkt XIV ust. 3.

XV. OPIS SPOSOBU PRZYGOTOWANIA I SKŁADANIA OFERT

1. Wykonawca może złożyć tylko jedną ofertę na każdą część postępowania.

2. Wykonawca składa ofertę za pośrednictwem „Formularza do złożenia, zmiany, wycofania oferty lub wniosku" dostępnego na ePUAP i udostępnionego również na miniPortalu. Funkcjonalność do zaszyfrowania oferty przez Wykonawcę jest dostępna dla wykonawców na miniPortalu, w szczegółach danego postępowania. W formularzu oferty Wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.

3. Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w szczególności w formacie danych: pdf, doc, docx, rtf, odt.

4. Ofertę składa się, pod rygorem nieważności, w formie elektronicznej.

5. Sposób złożenia oferty, w tym zaszyfrowania oferty opisany został w „Instrukcji użytkownika", dostępnej na stronie: https://miniportal.uzp.gov.pl/

6. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część należy ten plik zaszyfrować.

7. Ofertą składa się na formularzu ofertowym – zgodnie z załącznikiem nr 2 do SWZ. Wraz z ofertą wykonawca jest zobowiązany złożyć oświadczenia, o których mowa w pkt IX SWZ, zobowiązanie innego podmiotu, jeżeli wykonawca korzysta z zasobów innego podmiotu, pełnomocnictwo do reprezentowania w postępowaniu w przypadku wspólnego ubiegania się o udzielenie zamówienia bądź w przypadku podpisania oferty w imieniu Wykonawcy.

8. Oferta może być złożona tylko do upływu terminu składania ofert.

9. Wykonawca może przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem „Formularza do złożenia, zmiany, wycofania oferty lub wniosku" dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób wycofania oferty został opisany w „Instrukcji użytkownika" dostępnej na miniPortalu.

10. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

11. Oferta powinna być podpisana przez osobę upoważnioną/osoby upoważnione do reprezentowania Wykonawcy.

12. Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów rejestrowych (KRS, CEiDG lub innego właściwego rejestru), Wykonawca dołącza do oferty pełnomocnictwo. Pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

13. W przypadku gdy pełnomocnictwo zostało sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Przez cyfrowe odwzorowanie należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.

14. W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia do oferty należy załączyć pełnomocnictwo dla pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego na podstawie zasad określonych w pkt. XV ust. 12 i ust. 13 SWZ.

15. Podmiotowe środki dowodowe sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski.

16. Treść oferty musi odpowiadać treści SWZ.

XVI. TERMIN I MIEJSCE SKŁADANIA OFERT

Oferty wraz z dokumentami, o których mowa w SWZ powinny być przesłane do Zamawiającego na zasadach określonych w SWZ w terminie do 09.12.2021 r. do godz. 10:00.

XVII. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu 09.12.2021 r., o godzinie 10:15.
2. Otwarcie ofert nie jest publiczne, Wykonawcy nie mogą uczestniczyć w sesji otwarcia ofert.
3. Otwarcie ofert następuje poprzez użycie mechanizmu do odszyfrowania ofert dostępnego po zalogowaniu w zakładce Deszyfrowanie na miniPortalu i następuje poprzez wskazanie pliku do odszyfrowania.
4. Niezwłocznie po otwarciu ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje o:
   a) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   b) cenach lub kosztach zawartych w ofertach.

XVIII. OPIS SPOSOBU OBLICZANIA CENY

1. Przez cenę ofertową należy rozumieć cenę w rozumieniu art. 3 ust.1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz.U. z 2019, poz. 178)
2. W Formularzu oferty stanowiącym załącznik nr 2 do SWZ należy podać wartość netto za realizację zamówienia, do której, na potrzeby oceny ofert, należy dodać kwotę podatku VAT obliczoną wg właściwej stawki, których suma stanowić będzie cenę brutto (z podatkiem VAT) oraz wartość brutto za realizację całego zamówienia.
3. Cena ofertowa winna obejmować wszystkie koszty i składniki niezbędne do wykonania całości przedmiotu zamówienia w zakresie objętym opisem przedmiotu zamówienia oraz Wzorem umowy.
4. Cena ofertowa musi być wyrażona w złotych polskich (PLN). Rozliczenia za przedmiot zamówienia odbywać się będą w złotych polskich.
5. Podczas oceny oraz porównywania ofert złożonych w postępowaniu, Zamawiający będzie brał pod uwagę jedynie ceny brutto zgodnie z obowiązującą stawką VAT określoną na podstawie właściwych przepisów prawa.
6. W przypadku rozbieżności pomiędzy ceną wpisaną liczbowo oraz słownie, Zamawiający będzie brał pod uwagę jedynie ceny wpisane liczbowo.
7. Zamawiający nie przewiduje możliwości rozliczenia z Wykonawcą w innej walucie niż złoty polski.

XIX. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Zamawiający dokona oceny ofert, które nie zostały odrzucone, złożonych w poszczególnych zadaniach oraz dokona wyboru oferty najkorzystniejszej w danym zadaniu, spośród ofert spełniających wymagania określone w Załączniku nr 1 do SWZ – „Opis przedmiotu zamówienia", w oparciu o następujące kryteria i ich wagi:

1. Łączna cena oferty – 80 %
2. Czas dostawy (liczony do daty podpisania protokołu odbioru) – 20 %

Kryterium „Łączna cena oferty"

Ocena punktowa każdej oferty w kryterium „Łączna cena oferty" dokonana zostanie zgodnie z formułą:

liczba punktów = Cmin/Co x **80**

gdzie:
Cmin – najniższa łączna cena ofertowa brutto spośród złożonych ofert,
Co – cena brutto oferty ocenianej,

Kryterium czas dostawy na przedmiot zamówienia:

Dostawa do 4 tygodni – 20 pkt
Dostawa do 6 tygodni – 10 pkt
Dostawa do 8 tygodni – 0 pkt
Wymaga się podania czasu dostawy w PEŁNYCH tygodniach.

Sposób obliczania całkowitej liczby punktów dla danej oferty:
Całkowita liczba punktów dla danej oferty jest sumą przyznanych punktów dla wymienionych powyżej kryteriów.

Punktacja przyznawana oferentom w poszczególnych kryteriach będzie liczona z dokładnością do dwóch miejsc po przecinku. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.

2. W oparciu o powyższe kryteria opisane wzorem zostanie sporządzone zbiorcze zestawienie oceny ofert. Punkty będą liczone z dokładnością do dwóch miejsc po przecinku. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę spośród ofert spełniających wszystkie wymagania opisane w SWZ.
3. W przypadku braku możliwości wyboru najkorzystniejszej oferty ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i kryterium czas dostawy, Zamawiający spośród ofert wybierze ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia, w terminie określonym przez Zamawiającego, ofert dodatkowych, zawierających nową cenę.
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.

XX. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego z uwzględnieniem art. 577 ustawy PZP w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty przy użyciu środków komunikacji elektronicznej.
2. Zamawiający może zawrzeć umowę przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu złożono tylko 1 ofertę.
3. Wykonawca, o którym mowa w ust. 1 ma obowiązek zawrzeć umowę na warunkach określonych w projektowanych postanowieniach umowy, które stanowią załącznik do niniejszej SWZ.
4. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
5. Wykonawca przed zawarciem umowy zobowiązany jest do dostarczenia umowy regulującej współpracę wykonawców wspólnie ubiegających się o udzielenie zamówienia (w przypadku składania oferty wspólnej). Umowa taka winna określać strony umowy, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdemu z nich, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania konsorcjum (obejmującego okres realizacji przedmiotu zamówienia, gwarancji i rękojmi), wykluczenie możliwości wypowiedzenia umowy konsorcjum przez któregokolwiek z jego członków do czasu wykonania zamówienia.
6. Jeżeli wykonawca uchyla się od zawarcia umowy zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu albo unieważnić postępowanie.

XXI. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie żąda zabezpieczenia należytego wykonania umowy.

XXII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY

Wszelkie postanowienia umowy wraz z dopuszczalnymi zmianami umowy w sprawie zamówienia publicznego zostały zawarte we wzorze umowy stanowiącym załącznik nr 4 do SWZ.

XXIII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes prawny w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy pzp, przysługują środki ochrony prawnej przewidziane w Dziale IX tej ustawy.
2. Zgodnie z art. 513 ustawy Prawo zamówień publicznych odwołanie przysługuje na:
   a) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   b) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy;
3. Odwołanie wnosi się do Prezesa Izby
   a) Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
   b) Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
4. Odwołanie wnosi się w przypadku zamówień, których wartość jest mniejsza niż progi unijne, w terminie 5 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej.

5. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia publikacji ogłoszenia w Biuletynie Zamówień Publicznych lub zamieszczenia dokumentów zamówienia na stronie internetowej.
6. Odwołanie w przypadkach innych niż określone w pkt. XXIII ust. 4 i ust. 5 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

XXIV. POSTANOWIENIA DOTYCZĄCE JAWNOŚCI PROTOKOŁU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

1. Zamawiający udostępnia protokół lub załączniki do protokołu na wniosek.
2. Protokół wraz z załącznikami jest jawny.
3. Zasada jawności, o której mowa w ust. 2:
   a) ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zebranych w toku postępowania o udzielenie zamówienia.
   b) Ograniczenia zasady jawności, o których mowa w art. 74 ust. 3 ustawy pzp i art. 18 ust. 3-6 ustawy pzp, stosuje się odpowiednio
4. Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, Zamawiający nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 rozporządzenia 2016/679.
5. Przekazanie protokołu lub załączników następuje przy użyciu środków komunikacji elektronicznej.
6. W przypadku protokołu lub załączników sporządzonych w postaci papierowej, jeżeli z przyczyn technicznych znacząco utrudnione jest udostępnienie tych dokumentów przy użyciu środków komunikacji elektronicznej, w szczególności z uwagi na ilość żądanych do udostępnienia dokumentów, zamawiający informuje o tym wnioskodawcę i wskazuje sposób, w jaki mogą być one udostępnione.
7. Załączniki do protokołu postępowania udostępnia się po dokonaniu wyboru najkorzystniejszej oferty albo unieważnieniu postępowania, z tym że oferty wraz z załącznikami udostępnia się niezwłocznie po otwarciu ofert, nie później jednak niż w terminie 3 dni od dnia otwarcia ofert, przy czym nie udostępnia się informacji, które mają charakter poufny, w tym przekazywanych w toku negocjacji lub dialogu.
8. W sprawach nieuregulowanych zastosowanie mają przepisy ustawy Prawo zamówień publicznych.

ZAŁACZNIKI:

- Opis przedmiotu zamówienia — załącznik Nr 1
- Formularz ofertowy — załącznik Nr 2
- Oświadczenia Wykonawcy — załącznik Nr 3a i 3b
- Istotne warunki umowy — załącznik Nr 4
- Klauzula informacyjna RODO — załącznik Nr 5
- Wykaz podwykonawców — załącznik Nr 6

Załącznik Nr 1 do SWZ **Znak sprawy ZP.215.04.2021**

OPIS PRZEDMIOTU ZAMÓWIENIA

Część I

Przedmiotem zamówienia jest dostawa urządzenia typu UTM centralny wraz z niezbędnym oprogramowaniem i licencjami udzielonymi na okres co najmniej 60 miesięcy liczony od dnia podpisania protokołu odbioru urządzeń, oprogramowania ochrony poczty oraz trzech urządzeń typu firewall.

1. Przeprowadzenie prac związanych z migracją z posiadanych przez Zamawiającego urządzeń UTM (przeniesienie istniejących usług) na nowe dostarczone urządzenia.
2. Wykonanie dokumentacji projektowej, powykonawczej, eksploatacyjnej a także scenariuszy testów akceptacyjnych.
3. Przeprowadzenie ogólnego szkolenia z funkcjonowania i obsługi urządzeń.
4. Zapewnienie wsparcia technicznego na okres co najmniej 60 miesięcy liczony od dnia podpisania protokołu odbioru urządzeń
5. Wykaz prac:
   a) Wykonanie analizy istniejącego rozwiązania,
   b) Montaż i uruchomienie dostarczonych w ramach postępowania urządzeń,
   c) Podłączenie dostarczonych w ramach postępowania urządzeń,
   d) Przeniesienie i konfiguracja istniejących usług na dostarczone w ramach postępowania urządzenia,
   e) Uruchomienie mechanizmów ochrony przed awariami elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych,
   f) Uruchomienie mechanizmów bezpieczeństwa,
   g) Wykonanie testów akceptacyjnych,
   h) Wykonanie testów wydajnościowych urządzeń dostarczonych w ramach postępowania. Testy muszą wykazać spełnianie co najmniej minimalnych parametrów technicznych oferowanego sprzętu.
6. Dostawa dwóch voucherów na szkolenie w autoryzowanym ośrodku producenta dotyczące dostarczonego sprzętu ważne do końca roku 2022 do wykorzystania w różnych terminach na terenie kraju lub zdalnie. Szkolenie winno obejmować swoim zakresem:
   a) konfigurację tryb pracy urządzenia dla wybranej sieci,
   b) używanie GUI i CLI do zadań administracyjnych,
   c) tworzenia polityk zapory sieciowej
   d) konfiguracja uwierzytelnianiem użytkowników,
   e) konfiguracja SSL VPN,
   f) konfiguracja profili bezpieczeństwa,
   g) konfiguracja IPS, antywirus,
   h) filtrowanie ruchu www,
   i) zarządzanie aplikacjami do monitorowania i kontrolowania komunikacji sieciowej aplikacji,
   j) ochronę przed wyciekami danych, identyfikację plików z danymi wrażliwymi i sposoby blokady możliwość ich przesłania poza chronione sieci,
   k) analizę logów.

1. UTM centralny – 1 szt.

Nazwa ……

Model ……

Typ ……

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych	Spełnia (Tak/Nie)
1.	**Wymagania Ogólne**	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	
2.	**Redundancja, monitoring i wykrywanie awarii**	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	
3.	**Interfejsy, Dysk, Zasilanie**	1 .System realizujący funkcję Firewall musi dysponować minimum: • 18 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps.	

		2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.	
4.	**Parametry wydajnościowe**	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 250 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.	
5.	**Funkcje Systemu Bezpieczeństwa**	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.	
6.	**Polityki, Firewall**	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	

		2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	
7.	**Połączenia VPN**	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Routing i obsługa łączy WAN	
8.	**Routing i obsługa łączy WAN**	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	

9.	**Zarządzanie pasmem**	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	
10.	**Ochrona przed malware**	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
11.	**Ochrona przed atakami**	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
12.	**Kontrola aplikacji**	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	

		3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
13.	**Kontrola WWW**	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	
14.	**Uwierzytelnianie użytkowników w ramach sesji**	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: •Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. •Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. •Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
15.	**Zarządzanie**	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	

		3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
16.	**Logowanie**	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.	
17.	**Certyfikaty**	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
18.	**Serwisy i licencje**	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.	
19.	**Gwarancja oraz wsparcie**	System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

20.	**Rozszerzone wsparcie serwisowe**	System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.	
21.	**Oferent winien przedłożyć dokumenty**	•Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.	

2. System ochrony poczty.

Nazwa ……

Model ……

Typ ……

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych	Spełnia (Tak/Nie)
1.	**Wymagania ogólne**	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).	
2.	**Parametry fizyczne systemu antyspamowego**	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.	
3.	**Funkcja serwera poczty**	W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych. W tym zakresie dostarczony system musi zapewniać: 1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP. 2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).	

		3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników. 4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3). 5. Polski interfejs użytkownika przy dostępie przez WebMail. 6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP. 7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.	
4.	**Ogólne funkcje systemu ochrony poczty**	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 20 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail lub IMAP. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.	

		14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.	
5.	**Kontrola antywirusowa i ochrona przed malware**	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake.	
6.	**Kontrola antyspamowa**	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.	

		8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.	
7.	**Ochrona przed atakami na usługę poczty**	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. 4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.	
8.	**Funkcje logowania i raportowania**	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.	
9.	**Funkcje pracy w trybie wysokiej dostępności (HA)**	System ochrony poczty musi zapewniać poniższe funkcje: 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.	

10.	**Aktualizacje sygnatur, dostęp do bazy spamu**	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.	
11.	**Zarządzanie**	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.	
12.	**Certyfikaty**	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.	
13.	**Serwisy i licencje**	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 60 miesięcy.	
14.	**Gwarancja oraz wsparcie**	System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	

3. Urządzenie UTM o funkcjonalności firewall i z wbudowaną obsługą Wi-Fi – 3 szt.

Nazwa ……

Model ……

Typ ……

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych	Spełnia (Tak/Nie)
1.	**Wymagania Ogólne**	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	
2.	**Redundancja, monitoring i wykrywanie awarii**	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	
3.	**Interfejsy, Zasilanie:**	1. System realizujący funkcję Firewall musi dysponować minimum: • 5 portami Gigabit Ethernet RJ-45. • Ponadto system realizujący funkcje firewall musi być wyposażony w dwa interfejsy radiowe WiFi pracujące w standardach 802.11 a/b/g/n/ac. Jeżeli takiego interfejsu nie posiada, koniecznym jest dostarczenie urządzenia Access Point	

		pracującego w w.w. standardach radiowych wraz z systemem centralnego zarządzania siecią WiFi (kontrolerem). 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC.	
4.	**Parametry wydajnościowe**	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps. 5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.	
5.	**Funkcje Systemu Bezpieczeństwa**	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.	

		12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system	
6.	**Polityki, Firewall**	1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.	
7.	**Połączenia VPN**	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.	

		• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.	
8.	**Routing i obsługa łączy WAN**	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	
9.	**Funkcje SD-WAN**	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.	
10.	**Zarządzanie pasmem**	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	
11.	**Ochrona przed malware**	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	
12.	**Ochrona przed atakami**	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton,	

		Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
13.	**Kontrola aplikacji**	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
14.	**Kontrola WWW**	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	
15.	**Uwierzytelnianie użytkowników w ramach sesji**	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	

		4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	
16.	**Zarządzanie**	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
17.	**Logowanie**	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.	
18.	**Certyfikaty**	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
19.	**Serwisy i licencje**	W ramach postępowania Zamawiający chce pozyskać system z funkcjonalnościami firewall, nie jest wymagane dostarczenie licencji upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów jak np.: Kontrola Aplikacji, IPS, Antywirus.	

20.	**Gwarancja oraz wsparcie**	System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

Uwaga

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

Część II

I. Zamawiający posiada Microsoft Exchange Serwer 2016 CU22 zainstalowany na maszynie wirtualnej Windows Server 2016. Poziom lasu AD Windows Server 2016.

W ramach zamówienia Wykonawca dostarczy, przeprowadzi instalację i skonfiguruje redundantne rozwiązanie systemu poczty. Zamawiający wymaga dostarczenia:

- ExchgSvrStd 2019 SNGL OLP NL- 2 szt.
- ExchgStdCAL 2019 SNGL OLP NL UsrCAL- 125 szt.
- WinSvrSTDCore 2019 SNGL OLP 16Lic NL CoreLic- 2 szt.

1. Instalacja obejmuje:
   - przegląd Active Directory pod kątem przygotowania do migracji,
   - przegląd lokalnego Exchange'a pod kątem przygotowania do migracji,
   - konfiguracja redundantnego, odpornego na awarię systemu poczty elektronicznej,
   - Instalacja Systemów (system ma zostać oparty o wirtualne węzły, z których każdy ma być uruchomiony na oddzielnym fizycznym serwerze wirtualizacyjnym),
   - Instalacja Exchange Server,
   - Instalacja certyfikatu.
2. Konfiguracja obejmuje:
   - Rozwiązanie ma być tak skonfigurowane, aby każdy z serwerów wchodzący w skład klastra był w stanie samodzielnie obsłużyć cały ruch pocztowy w przypadku awarii drugiego węzła),
   - Rozwiązanie powinno rozkładać obciążenie między węzły klastra.
3. Migracja obejmuje:
   - W ramach usługi Wykonawca musi wykonać migrację skrzynek oraz poczty ze starego serwera na nowe rozwiązanie.
   - W ramach usługi Wykonawca musi wykonać migrację folderów publicznych ze starego serwera na nowe rozwiązanie.
   - W ramach usługi Wykonawca musi wykonać migrację grup dystrybucyjnych ze starego serwera na nowe rozwiązanie.
4. Weryfikacja wykonanych czynności:
   - Weryfikacja migracji,
   - Test działania środowiska pocztowego, weryfikacja przejęcia działania całego środowiska przez pojedynczy serwer Exchange.

Całość prac związana z wdrożeniem nowego rozwiązania nie powinna powodować przerw w działaniu dotychczasowego rozwiązania do momentu całkowitego przełączenia się na nowe serwery i wyłączenia starego systemu.

Załącznik Nr 2 do SWZ **Znak sprawy ZP.215.04.2021**

Formularz ofertowy

Nazwa oferenta .....

Adres oferenta .....

NIP ……. REGON ……...

Numer telefonu ..... e-mail ……

Adres skrzynki ePUAP .....

OFERTA
NA DOSTAWĘ SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA

Składając ofertę w postępowaniu o zamówienie publiczne prowadzonym w trybie podstawowym bez negocjacji na dostawę sprzętu komputerowego i oprogramowania do Polskiego Radia Białystok S.A. (znak sprawy: ZP.215.04.2021), oferujemy wykonanie zamówienia za cenę:

Oferujemy wykonanie zamówienia zgodnie z postanowieniami SWZ przedmiotowego postępowania za cenę:

Nr części	Nazwa	Kwota netto	Podatek VAT	Kwota brutto
Część 1				
Część 2				

Termin wykonania umowy (w tygodniach) od daty podpisania umowy:

Część 1 ……..

Część 2 ……..

1. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
2. Oświadczamy, że uzyskaliśmy od Zamawiającego wszelkie informacje niezbędne do rzetelnego sporządzenia i skalkulowania niniejszej oferty zgodnie z wymogami określonymi w specyfikacji warunków zamówienia.
3. Oświadczamy, że podana cena brutto zawiera wszelkie koszty, jakie ponosi Zamawiający w przypadku wyboru naszej oferty.
4. Oświadczamy, że zawarty w SWZ wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na zawartych w nim warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.
5. Zobowiązujemy się wykonać przedmiot zamówienia zgodnie z treścią i wymogami SWZ.

6. Oświadczamy, że niniejsza oferta zawiera w następujących załącznikach: …….. informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji /jeżeli dotyczy/.
7. Oświadczamy, że związani jesteśmy niniejszą ofertą przez okres 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem związania ofertą jest dzień, w którym upływa termin składania ofert.
8. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dni 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu *(jeżeli dotyczy, jeżeli nie dotyczy skreślić).*
9. Osobami uprawnionymi do kontaktów z Zamawiającym są:

1) …… tel. …… e-mail ……
2) …… tel. …… e-mail ……

10. Świadomy odpowiedzialności karnej wynikającej z art. 297 k.k. oświadczamy, że załączone do oferty dokumenty opisują stan faktyczny i prawny aktualny na dzień ich złożenia.
11. Wraz z ofertą składamy następujące dokumenty i oświadczenia:
    1) oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu oraz o niepodleganiu wykluczeniu
    2) opis oferowanych urządzeń zgodnie z załącznikiem nr 1 do SWZ,
    3) zestawienie oferowanego sprzętu komputerowego i oprogramowania wg. wzoru (wraz z cenami jednostkowymi)
    4) ……

Zestawienie oferowanego sprzętu komputerowego i oprogramowania (wraz z cenami jednostkowymi)

Część 1

Lp.	Nazwa, typ, model	Ilość	Cena netto (szt.)	Wartość netto	Wartość brutto
1					
2					
3					
…					

Część 2

Lp.	Nazwa, typ, model	Ilość	Cena netto (szt.)	Wartość netto	Wartość brutto
1					
2					
3					
…					

Oświadczam(y), że Wykonawca, którego reprezentuję(emy) jest:

- ☐ mikro przedsiębiorcą
- ☐ małym przedsiębiorcą (małe przedsiębiorstwo definiuje się jako przedsiębiorstwo, które zatrudnia mniej niż 50 pracowników i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR)

- ☐ średnim przedsiębiorcą (średnie przedsiębiorstwo definiuje się jako przedsiębiorstwo, które zatrudnia mniej niż 250 pracowników i którego roczny obrót nie przekracza 50 milionów lub roczna suma bilansowa nie przekracza 43 milionów EUR)
- ☐ jednoosobową działalnością gospodarczą
- ☐ osobą fizyczną nieprowadzącą działalności gospodarczej
- ☐ inny rodzaj

....

(Miejscowość i data) (Podpis wykonawcy lub upełnomocnionego przedstawiciela wykonawcy)

Załącznik Nr 3a do SWZ **Znak sprawy ZP.215.04.2021**

Nazwa oferenta .....

Adres oferenta .....

NIP …… REGON ……...

Numer telefonu ..... e-mail ……

Oświadczenie Wykonawcy o spełnieniu warunków udziału w postępowaniu oraz o niepodleganiu wykluczeniu, o którym mowa w art. 125 ust. 1 ustawy pzp

Na potrzeby prowadzonego postępowania, którego przedmiotem jest dostawa sprzętu komputerowego i oprogramowania do Polskiego Radia Białystok S.A. (Znak sprawy ZP.215.04.2021) oświadczam, że:

Oświadczenie o spełnianiu warunków:

Oświadczam, że Wykonawca ……

spełnia warunki udziału w postępowaniu określone przez Zamawiającego w pkt. VIII Specyfikacji Warunków Zamówienia.

Oświadczenie o niepodleganiu wykluczeniu:
Oświadczam, że Wykonawca nie podlega wykluczeniu na podstawie:
- art. 108 ust. 1 pkt 1-6 ustawy;
- art. 109 ust. 1 pkt. 4, 5, 7 ustawy.

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

....
(Miejscowość i data) (Podpis wykonawcy lub upełnomocnionego przedstawiciela wykonawcy)

Załącznik Nr 3b do SWZ **Znak sprawy ZP.215.04.2021**

Nazwa oferenta .....

Adres oferenta .....

NIP ……. REGON ……...

Numer telefonu ..... e-mail ……

Oświadczenie Wykonawcy o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 108 ust. 1 pkt 5 ustawy pzp

Na potrzeby prowadzonego postępowania, którego przedmiotem jest dostawa sprzętu komputerowego i oprogramowania do Polskiego Radia Białystok S.A. (Znak sprawy ZP.215.04.2021) oświadczam, że:

1. Przynależę/ nie przynależę***** do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 roku o ochronie konkurencji i konsumentów (Dz. U z 2015 r. poz. 184, 1616 i 1634) z innymi wykonawcami, którzy złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w niniejszym postępowaniu.

2. Wykaz wykonawców należących do tej samej grupy kapitałowej, którzy złożyli oferty:
   .....

3. Oświadczam, że w przypadku przynależenia do tej samej grupy kapitałowej powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w przedmiotowym postępowaniu**.** W załączeniu przekazujemy informacje, potwierdzające przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

***** Niepotrzebne skreślić

....

(Miejscowość i data) (Podpis wykonawcy lub upełnomocnionego przedstawiciela wykonawcy)

Załącznik Nr 4 do SWZ **Znak sprawy ZP.215.04.2021**

Istotne warunki umowy (dotyczy części 1 przedmiotu zamówienia)

zawarta w Białymstoku ……. 2021 r. pomiędzy:

Polskim Radiem – Regionalną Rozgłośnią w Białymstoku „Radio Białystok" Spółką Akcyjną z siedzibą w Białymstoku (15-328) przy ul. Świerkowej 1, wpisaną do Krajowego Rejestru Sądowego w Sądzie Rejonowym w Białymstoku XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000037873, z kapitałem zakładowym 783 300,00 zł wpłaconym w całości, REGON: 050252837, NIP: 542-00-03-367, zwaną dalej "**Zamawiającym**", reprezentowaną przez:
Wojciecha Straszyńskiego – Prezesa zarządu
a
……

……

zwanym dalej „**Wykonawcą**" reprezentowanym przez:
…….

łącznie zwanymi "Stronami"

§ 1.

1. Przedmiotem Umowy jest dostawa na rzecz Zamawiającego sprzętu komputerowego zgodnie ze Szczegółowym Opisem Przedmiotu Zamówienia (Tabela techniczna zamówienia) stanowiącym załącznik nr 2 do Umowy. Wykonawca dostarczy do siedziby Zamawiającego sprzęt komputerowy wraz z licencjami. Przedmiot Umowy zwany jest dalej również „sprzętem" lub „przedmiotem zamówienia".
2. Wykonawca zapewni również świadczenie usług serwisu, napraw gwarancyjnych, konsultacji i pomocy technicznej dot. przedmiotu Umowy przez okres i na zasadach określonych w Umowie i załączniku nr 2.

§ 2.

1. Wykonawca oświadcza, że parametry techniczne i użytkowe sprzętu są zgodne ze złożoną ofertą w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, znak: ZP 215.04.2021, a dostarczony sprzęt stanowi jego wyłączną własność, jest fabrycznie nowy, nieużywany i jest zgodny z dostarczoną dokumentacją oraz spełnia wymogi w zakresie bezpieczeństwa wynikające z ustawy o systemie oceny zgodności. Przez stwierdzenie „fabrycznie nowy" należy rozumieć sprzęt nieużywany, oryginalnie opakowany (tzn. wyprodukowany nie dawniej niż na 6 miesięcy przed jego dostarczeniem).
2. Wykonawca odpowiada za wady fizyczne i prawne dostarczonego sprzętu.
3. Wykonawca oświadcza, że przedmiot Umowy jest wolny od jakichkolwiek wad fizycznych i prawnych oraz roszczeń osób trzecich. Przez wadę fizyczną należy rozumieć również jakąkolwiek niezgodność sprzętu ze szczegółowym opisem przedmiotu zamówienia.
4. Wykonawca dostarczy przedmiot Umowy na własny koszt, własnym staraniem i na własne ryzyko do siedziby Radia Białystok ul. Świerkowa 1 15-328 w godz. 9.00-15.00 w dniu roboczym.
5. Upoważniony przedstawiciel Zamawiającego sprawdzi zgodność dostawy sprzętu w siedzibie Zamawiającego.
6. Do potwierdzenia wykonania przedmiotu Umowy niezbędne jest protokolarne przekazanie przez Wykonawcę przedmiotu Umowy wraz z dokumentami gwarancyjnymi i instrukcjami obsługi w języku polskim lub angielskim Zamawiającemu i dokonanie przez Zamawiającego odbioru bez zastrzeżeń. Wzór protokołu odbioru stanowi Załącznik nr 1 do Umowy.

7. W przypadku niezgodności przedmiotu Umowy, pod względem ilości, rodzaju lub stwierdzenia innych wad podczas odbioru, Wykonawca zobowiązany jest niezwłocznie, nie przekraczając terminu, o którym mowa w §3 ust. 1, dostarczyć na własny koszt sprzęt wolny od wad i zgodny z przedmiotem Umowy.
8. Wykonawca udziela Zamawiającemu gwarancji na sprzęt zgodnie z załącznikiem nr 2.
9. Okres gwarancji liczony jest od daty odbioru przedmiotu Umowy wskazanego w protokole odbioru podpisanym bez zastrzeżeń.
10. Zakres usług gwarancyjnych obejmuje w szczególności:
   – naprawy, w tym usuwanie usterek, wymiany gwarancyjne uszkodzonych elementów lub sprzętu, w miejscu dostawy sprzętu, konsultacje i pomoc techniczną w zakresie funkcjonowania sprzętu,
   – dostęp do najnowszych sterowników i uaktualnień na stronach producenta sprzętu oraz poprawek i aktualizacji oprogramowania dostarczanego wraz ze sprzętem,
   – przyjmowanie zgłoszeń wadliwego działania sprzętu,
   – diagnozę sprzętu,
   – dojazdy i transport niezbędny do wykonania czynności serwisowych ,
   – przeprowadzenie niezależnej ekspertyzy, o której mowa w ust. 11 pkt 10,
   – inne czynności niezbędne do realizacji uprawnień wynikających z gwarancji.
11. Warunki serwisu gwarancyjnego:
   1) Czas reakcji serwisu (podjęcie czynności w celu usunięcia usterki) na zgłoszenie usterki wynosi 8 godzin od momentu jej zgłoszenia. Zgłoszenia usterek Zamawiający będzie dokonywał:
      a) faksem na nr …….. (data zgłoszenia usterki), przy czym potwierdzenie prawidłowej transmisji faksu jest dowodem na zgłoszenie usterki. Wykonawca potwierdzi tego samego dnia faksem na nr 85 744 34 23 przyjęcia zgłoszenia o usterce.
      b) e-mailem na adres: …… Wykonawca każdorazowo musi potwierdzić zwrotnie drogą elektroniczną fakt otrzymania zgłoszenia w przeciągu maksymalnie 12 godzin od jego otrzymania.
   2) Gwarancja na dostarczony przedmiot umowy liczona jest od daty jego dostawy do Wykonawcy.
   3) W przypadku konieczności dokonania naprawy w innym miejscu niż miejsce używania przedmiotu umowy, koszt i odpowiedzialność za jego transport ponosi Wykonawca od chwili wydania wadliwego przedmiotu umowy jego upoważnionemu przedstawicielowi do chwili odbioru przedmiotu umowy przez upoważnionego przedstawiciela Zamawiającego po dokonaniu naprawy.
   4) W przypadku przekroczenia terminu naprawy, który strony ustalają na 14 dni roboczych, Wykonawca jest zobowiązany do wymiany sprzętu na nowy o takich samych lub wyższych parametrach technicznych, uzgodnionych z Zamawiającym w miejsce sprzętu uszkodzonego, z zastrzeżeniem ustaleń ust. 6.
   5) Jeżeli czas naprawy sprzętu określonego w § 1 z przyczyn niezależnych od Wykonawcy będzie dłuższy niż 14 dni roboczych, Wykonawca zobowiązany jest wykazać te przyczyny odpowiednimi dokumentami, a Zamawiający może ponownie ustalić termin naprawy sprzętu.
   6) W przypadku zaistnienia konieczności dokonania czwartej naprawy sprzętu, Wykonawca wymieni sprzęt na nowy egzemplarz wolny od wad.
   7) Wykonawca gwarantuje, że usługi objęte przedmiotem Umowy będą świadczone przez producenta lub autoryzowanego partnera serwisowego sprzętu, w sposób profesjonalny, zgodnie ze standardami obowiązującymi w branży informatycznej, z zachowaniem należytej staranności,
   8) Wykonawca ponosi wszelkie koszty i ryzyko związane z realizacją uprawnień gwarancyjnych przez Zamawiającego w okresie gwarancji,
   9) w razie nieuwzględnienia przez Wykonawcę reklamacji z tytułu gwarancji, Zamawiający może wystąpić do podmiotu trzeciego z wnioskiem o przeprowadzenie niezależnej ekspertyzy; jeżeli reklamacja Zamawiającego okaże się uzasadniona, koszty związane z przeprowadzeniem ekspertyzy ponosi Wykonawca. Zwrot kosztów ekspertyzy nastąpi w terminie 14 dni kalendarzowych, od dnia otrzymania przez Wykonawcę wezwania do zapłaty,
   10) uprawnienia wynikające z udzielonej gwarancji nie wyłączają możliwości dochodzenia przez Zamawiającego uprawnień z rękojmi za wady,
   12) świadczenie na rzecz Zamawiającego usług gwarancyjnych i serwisowych oraz korzystanie z uprawnień wynikających z gwarancji zawarte jest w wynagrodzeniu Wykonawcy, o którym mowa w § 4 ust. 1.

12. Wykonawca odpowiada dodatkowo z tytułu rękojmi za wady na zasadach wynikających z Kodeksu cywilnego przez okres równy okresowi gwarancji.

§ 3.

1. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy, o którym mowa w §1 ust. 1, w terminie do …….. 2021 r.
2. Za termin realizacji przedmiotu Umowy przyjmuje się wskazaną, w podpisanym przez Strony bez zastrzeżeń protokole odbioru, datę wykonania bez wad całości przedmiotu Umowy, o którym mowa w §1 ust. 1.
3. Usługi objęte przedmiotem Umowy, o których mowa w § 1 ust. 2 Umowy świadczone będą przez okres wskazany w § 2 ust. 8.
4. Jeżeli termin na wykonanie zobowiązania kończy się w sobotę lub dzień ustawowo wolny od pracy przyjmuje się, że termin upływa następnego dnia roboczego.

§ 4.

1. Wynagrodzenie Wykonawcy z tytułu realizacji przedmiotu umowy wynosi: ……. zł brutto (słownie złotych: …… ……), w tym VAT …….. zł (słownie złotych: ……..), netto …….. zł (słownie złotych: ……..)..
2. Ceny jednostkowe brutto sprzętu zawiera formularz stanowiący Załącznik nr 3 do Umowy.
3. Wykonawcy przysługuje wynagrodzenie za przedmiot Umowy dostarczony i odebrany protokolarnie przez Zamawiającego bez zastrzeżeń.
4. Wynagrodzenie Wykonawcy, o którym mowa w ust. 1, jest ostateczne i obejmuje wszystkie koszty i opłaty towarzyszące wykonaniu Umowy, jakie mogą powstać w związku z jej realizacją, w tym koszty opłat pośrednich, celnych, podatek od towarów i usług (VAT), ubezpieczenie, koszt transportu, załadunku i rozładunku, koszty wymiany wadliwego przedmiotu zamówienia na pozbawiony wad, koszty odbioru i dostarczenia elementów podlegających wymianie gwarancyjnej, koszty serwisu gwarancyjnego, opłat licencyjnych oraz inne usługi/koszty związane z wykonaniem przedmiotu zamówienia, etc.

§ 5.

1. Należność za dostarczony sprzęt i oprogramowanie płatna będzie przelewem na rachunek bankowy Wykonawcy wskazany na „Białej liście" podatników VAT na stronie internetowej Ministerstwa Finansów w terminie do 14 dni kalendarzowych od dnia otrzymania prawidłowo wystawionej przez Wykonawcę faktury.
2. Za dzień zapłaty ustala się dzień wydania dyspozycji dokonania przelewu bankowi prowadzącemu rachunek Zamawiającego
3. Strony zobowiązują się do wzajemnego informowania o wszelkich zmianach danych, które mogą wpływać na wystawianie i obieg faktur oraz ich księgowanie i rozliczanie dla celów podatkowych, takich jak nazwa, adres, numer rachunku bankowego, NIP itp.
4. Podstawą do wystawienia faktury jest protokół odbioru podpisany przez Zamawiającego bez zastrzeżeń.
5. Wykonawca zobowiązany jest wystawiać na Zamawiającego faktury wynikające z realizacji Umowy i przekazać je Zamawiającemu, zgodnie z jego wyborem w formie papierowej lub elektronicznej:
   a) dla faktur w formie papierowej: faktura zostanie wystawiona na Zamawiającego, tj. Polskie Radio – Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A., ul. Świerkowa 1, 15-328 Białystok, NIP 542-00-03-367, i zaadresowana: Polskie Radio – Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A., ul. Świerkowa 1, 15-328 Białystok;
   b) dla faktur w formie elektronicznej: faktura zostanie wystawiona na Zamawiającego, tj.: Polskie Radio – Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A., ul. Świerkowa 1, 15-328 Białystok, NIP 542-00-03-367 i przekazana w formie elektronicznej z poczty elektronicznej Wykonawcy ..... na adres poczty elektronicznej Zamawiającego: sekretariat@radio.bialystok.pl

6. W przypadku przekazywania faktur w formie elektronicznej, zgodnie z ust. 5 pkt b), Wykonawca zobowiązuje się złożyć stosowane oświadczenie przed wystawieniem faktury.
7. Zmiana adresów poczty elektronicznej wskazanych w ust. 5 pkt b) wymaga złożenia pisemnego oświadczenia, przy czym oświadczenie o dokonaniu zmiany przez Wykonawcę powinno zostać przedłożone Zamawiającemu przed wysłaniem faktury.
8. Wysłanie faktury z innego, niż wskazany w ust. 5 pkt b), adresu poczty elektronicznej, bez uprzedniego złożenia powyższego oświadczenia, o którym mowa w ust. 7, zwalania Zamawiającego z odpowiedzialności w przypadku braku zapłaty lub opóźnienia w zapłacie należności wynikającej z danej faktury.
9. W przypadku opóźnienia w zapłacie kwoty wynikającej z faktury, w sytuacji innej niż wskazana w ust. 8, Wykonawca jest uprawniony do żądania zapłaty przez Zamawiającego odsetek stosownie do obowiązujących przepisów za każdy dzień opóźnienia.

§ 6.

1. Wykonawca zapłaci Zamawiającemu następujące kary umowne:
   1) w wysokości 10% kwoty brutto, o której mowa w § 4 ust. 1, gdy Zamawiający odstąpi od Umowy w całości lub w części z przyczyn leżących po stronie Wykonawcy, w szczególności z przyczyn wymienionych w § 7 ust. 1 pkt 1 - 5 oraz § 7 ust. 3 .
   2) w wysokości 0,5 % kwoty brutto, o której mowa w § 4 ust. 1 za każdy rozpoczęty dzień roboczy zwłoki w realizacji przedmiotu Umowy w terminie, o którym mowa w § 3 ust.1,
2. W przypadku odstąpienia przez Zamawiającego od części Umowy Wykonawcy przysługuje wynagrodzenie jedynie za prawidłowo wykonaną, potwierdzoną przez Zamawiającego część Umowy.
3. Jeżeli na skutek niewykonania lub nienależytego wykonania części lub całości przedmiotu Umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną bądź szkoda powstanie z innych przyczyn niż te, dla których zastrzeżono kary umowne, Zamawiającemu przysługuje prawo do dochodzenia odszkodowań uzupełniających na zasadach ogólnych Kodeksu cywilnego.
4. Zapłata kar umownych, o których mowa w ust. 1 pkt 2 nie zwalnia Wykonawcy od obowiązku wykonania Umowy.
5. Zamawiający ma prawo do potrącenia z wartości wynagrodzenia za wykonanie przedmiotu Umowy wartości naliczonych kar, a w przypadku niedokonania potrącenia kara umowna jest płatna w terminie do 14 dni kalendarzowych, od daty otrzymania przez Wykonawcę wezwania do jej zapłaty.
6. Kary umowne podlegają sumowaniu.

§ 7.

1. Zamawiający zastrzega sobie prawo odstąpienia od całości lub części niezrealizowanej Umowy ze skutkiem natychmiastowym (bez wyznaczania Wykonawcy dodatkowego terminu w tym zakresie) w następujących okolicznościach:
   1) w przypadku, gdy Wykonawca nie wykona przedmiotu Umowy w terminie, o którym mowa w § 3 ust. 1,
   2) w przypadku zwłoki Wykonawcy w wykonaniu innych zobowiązań objętych Umową, przekraczającej 7 dni kalendarzowych,
   3) niedostarczenia sprzętu fabrycznie nowego,
   4) innego rodzaju nienależytego wykonania lub niewykonania Umowy, czyniącego dalsze jej realizowanie bezprzedmiotowym,
   5) gdy otwarto likwidację majątku Wykonawcy,
   6) w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
2. Zamawiający może odstąpić od Umowy na podstawie ust. 1 pkt 1-5 w terminie 30 dni od dnia powzięcia przez Zamawiającego wiadomości o zaistnieniu przyczyny do odstąpienia.
3. Zamawiający może również odstąpić od Umowy w całości lub w części w innych sytuacjach przewidzianych w Kodeksie cywilnym.
4. Odstąpienie od Umowy wymaga formy pisemnej.

§ 8.

1. Wykonawca nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na rzecz osób trzecich bez pisemnej zgody Zamawiającego.
2. Zamawiający dopuszcza zmianę postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w zakresie:
   1) w przypadku wycofania z rynku lub braku dostępności na rynku zaoferowanego sprzętu, dopuszcza się dostarczenie przez Wykonawcę innego sprzętu o parametrach i funkcjonalnościach nie gorszych niż wynikające z oferty; warunki dostawy oraz warunki wykonywania świadczeń gwarancyjnych pozostają bez zmian; wynagrodzenie Wykonawcy nie może ulec zwiększeniu,
   2) innych zmian, w zakresie dopuszczonym art. 144 ustawy Pzp.
3. Zmiany wskazane w ust. 2 wymagają formy pisemnej w postaci aneksu, pod rygorem nieważności. W przypadku zmian wskazanych w ust. 2 pkt. 1 Wykonawca dodatkowo zobowiązany jest do przedstawienia Zamawiającemu informacji o proponowanej zmianie wraz z wyjaśnieniem przyczyn proponowanej zmiany i uprawdopodobnieniem zajścia przesłanek uprawniających do zmiany.

§ 9.

1. Wykonawca oświadcza i gwarantuje, że zawarcie Umowy przez Wykonawcę, jej wykonanie, oraz korzystanie z licencji przez Zamawiającego zgodnie z Umową, nie narusza praw własności intelektualnej producenta oprogramowania, ani jakichkolwiek innych osób trzecich, w tym praw autorskich lub patentów.
2. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z Umową, w szczególności zarzucających naruszenie praw własności intelektualnej, Wykonawca podejmie wszelkie działania mające na celu zażegnanie sporu i poniesie w związku z tym wszelkie koszty od chwili wystąpienia przez osobę trzecią z roszczeniem wobec Zamawiającego, w tym koszty procesu, zastępstwa procesowego oraz odszkodowań. W szczególności, w razie wytoczenia przeciwko Zamawiającemu powództwa z tytułu naruszenia praw własności intelektualnej, Wykonawca wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie Zamawiającego.
3. Jeżeli wskutek orzeczenia sądu Zamawiający nie będzie mógł korzystać z przedmiotu Umowy, Wykonawca, na swój koszt i według własnego wyboru, uzyska dla Zamawiającego prawa do przedmiotu Umowy lub dokona wymiany na przedmiot nie naruszający praw. W przypadku jeżeli powyższe okaże się niemożliwe, Wykonawca będzie zobowiązany do zwrotu Zamawiającemu zapłaconego przez Zamawiającego wynagrodzenia.

§ 10.

1. Wykonawca i Zamawiający zobowiązują się do zapewnienia prawidłowego przetwarzania, udostępnionych przez drugą stronę, danych osobowych poprzez stosowanie odpowiednich organizacyjnych i technicznych środków ochrony tych danych, gwarantujących ochronę praw osób, których te dane dotyczą, zgodnie z przepisami i wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO), zapisami Ustawy z dnia 10.05.2018 r. o ochronie danych osobowych z późniejszymi zmianami (Dz. U. z 2018 r. poz.1000) lub innymi przepisami prawa polskiego, a w szczególności zobowiązują się jako podmiot przetwarzający do przestrzegania obowiązków wynikających z art. 28 i nast. wspomnianego rozporządzenia.
2. Na podstawie niniejszej umowy Wykonawca powierza Zamawiającemu przetwarzanie (w szczególności zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, wykorzystywanie, przesyłanie, usuwanie, niszczenie) następujących kategorii danych osobowych: imię i nazwisko oraz funkcja lub stanowisko osób reprezentujących Wykonawcę, imię i nazwisko osób wykonujących prace w ramach realizacji przedmiotu umowy, jeżeli przekazanie tych danych będzie konieczne w związku z realizacją przedmiotu umowy oraz osób wskazanych do kontaktu w związku z realizacją przedmiotu umowy przez okres trwania niniejszej umowy, a także adres e-mail lub telefon osób wskazanych do kontaktu.

Charakter przetwarzania danych dotyczy przetwarzania danych osobowych w formie papierowej i przy wykorzystaniu systemów informatycznych.

3. Na podstawie niniejszej umowy Zamawiający powierza Wykonawcy przetwarzanie (w szczególności zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, wykorzystywanie, przesyłanie, usuwanie, niszczenie) następujących kategorii danych osobowych: imię i nazwisko oraz funkcja lub stanowisko osób reprezentujących Zamawiającego oraz, imię i nazwisko osób wskazanych do kontaktu w związku z realizacją przedmiotu umowy, przez okres trwania niniejszej umowy, a także adres e-mail lub telefon osób wskazanych do kontaktu. Charakter przetwarzania danych dotyczy przetwarzania danych osobowych w formie papierowej i przy wykorzystaniu systemów informatycznych.
4. Wykonawca zobowiązuje się do zapoznania swoich współpracowników (niezależnie od podstawy prawnej współpracy) oraz podmiotów, za pośrednictwem, których realizować będzie niniejszą umowę z zasadami i procedurami związanymi z ochroną danych osobowych, w zakresie, w jakim te zasady i procedury będą miały wpływ na realizację umowy.
5. Strona przetwarzająca powierzone dane, przetwarza je zgodnie z poleceniem drugiej strony (administratora danych) i jest uprawniona do upoważnienia poszczególnych osób do przetwarzania ich w takim zakresie. Jednocześnie podmiot przetwarzający zapewni, by osoby upoważnione do przetwarzania danych osobowych zobowiązane były do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
6. Strona, której powierzono przetwarzanie danych po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki zgłasza je drugiej stronie (administratorowi), nie później niż w ciągu 24 godzin od stwierdzenia naruszenia poprzez: telefoniczny kontakt Zamawiającego 85 745 62 20 lub mailem na adres sekretariat@radio.bialystok.pl, telefoniczny kontakt Wykonawcy ……. lub mailem na adres ……...
7. Wykonawca i Zamawiający oświadczają, że dane osobowe, o których mowa w ust. 2-3, zostaną wykorzystane wyłącznie w celu realizacji przedmiotu umowy.
8. Wykonawca i Zamawiający zobowiązują się do przekazania lub trwałego zniszczenia we własnym zakresie (zgodnie z decyzją administratora), niezwłocznie po zakończeniu realizacji Umowy, ewentualnych dokumentów, ich kopii lub nośników zawierających dane osobowe, o których mowa w ust. 2-3, przy uwzględnieniu terminów obowiązkowego przechowywania dokumentów wynikających z obowiązujących przepisów.
9. Odpowiednio każda ze stron jako administrator zobowiązuje się i oświadcza, że będzie wypełniała obowiązki informacyjne przewidziane w art. 13 lub 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskała w celu realizacji przedmiotu umowy, a druga strona zobowiązuje się do współpracy w zakresie wykonania tego obowiązku.

§ 11.

Obowiązek informacyjny w związku z przetwarzaniem danych osobowych:

1. Administratorem danych osobowych jest Radio Białystok S.A. (dalej: „ADMINISTRATOR”), z siedzibą: ul. Świerkowa 1, 15-328 Białystok. Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: ul. Świerkowa 1, 15-328 Białystok lub drogą e-mailową pod adresem: iodo@radio.bialystok.pl.
2. Administrator wyznaczył Inspektora Ochrony Danych – Andrzeja Rybus-Tołłoczko, z którym można się skontaktować pod adresem mailowym: iodo@radio.bialystok.pl.
3. Pani/Pana dane osobowe są przetwarzane na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.
4. Przetwarzanie danych odbywa się w związku z:
   a) realizacją umowy na zlecone zamówienie publiczne – art. 6 ust. 1 lit. b RODO;

b) rozliczeniem umowy – art. 6 ust. 1 lit. c RODO;
c) realizacją zadania publicznego w ramach zamówienia publicznego – art. 6 ust. 1 lit. e RODO;
d) dochodzeniem i obroną roszczeń – art. 6 ust. 1 lit. f RODO,

5. Dane osobowe nie pochodzą od stron trzecich.
6. Administrator nie zamierza przekazywać danych do państwa trzeciego lub organizacji międzynarodowej.
7. Administrator nie zamierza przekazywać danych osobowych, a jeżeli musiałoby to nastąpić, to tylko na podstawie przepisów prawa, w tym do Urzędu Zamówień Publicznych, Organów Kontrolnych lub umowy powierzenia przetwarzania danych osobowych, w tym do dostawców usług teleinformatycznych, biur rachunkowych świadczących usługi na rzecz Administratora.
8. Dane będą przetwarzane przez okres 10 lat od początku roku następującego po roku, w którym nastąpiła realizacja zamówienia.
9. Osoba, której dane dotyczą ma prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
10. Skargę na działania Administratora można wnieść do Prezesa Urzędu Ochrony Danych Osobowych.
11. Podanie danych osobowych jest wymogiem prawa. Ich nie podanie spowoduje brak możliwości zawarcia umowy na realizację zamówienia publicznego, a co za tym idzie odstąpienie od jego realizacji.
12. Administrator nie przewiduje zautomatyzowanego podejmowania decyzji.

§ 12.

1. Na potrzeby niniejszej umowy przez dni robocze strony rozumieją dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
2. We wszystkich sprawach nieuregulowanych w niniejszej Umowie zastosowanie mają przepisy prawa polskiego, w szczególności przepisy:
   a) ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny,
   b) ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.
3. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Strony będą dążyły do polubownego rozstrzygania wszystkich sporów powstałych w związku z wykonywaniem niniejszej Umowy. W przypadku nieosiągnięcia porozumienia w drodze negocjacji, wszelkie spory rozstrzygane będą przez sąd miejscowo właściwy dla siedziby Zamawiającego.
5. Osoby wyznaczone do uzgodnień i koordynacji przedmiotu niniejszej Umowy:
   1) ze strony Zamawiającego – Jarosław Dobrowolski
   2) ze strony Wykonawcy – ……
6. Osobami upoważnionymi do podpisania protokołów odbioru:
   – ze strony Zamawiającego są: Jarosław Dobrowolski lub inne osoby upoważnione przez Zamawiającego,
   – ze strony Wykonawcy jest: ……
7. Zmiana osób, o których mowa w ust. 5 lub 6 może nastąpić po poinformowaniu drugiej strony i nie wymaga sporządzenia aneksu do Umowy.
8. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Załączniki:
Załącznik nr 1 – Wzór protokołu odbioru
Załącznik nr 2 – Tabela techniczna zamówienia
Załącznik nr 3 – Formularz cen jednostkowych

…… ……

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 protokół odbioru do umowy z dnia …….. 2021r.

PROTOKÓŁ ODBIORU

dotyczący realizacji postanowień umowy z dnia ……. 2021 do postępowania nr ZP.215.04.2021 na usługę dostawy:

- sprzętu komputerowego

Wykonawca	**Zleceniodawca**
	Polskie Radio - Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A. 15-328 Białystok ul. Świerkowa 1 NIP 542-00-03-367

Opis	Uwagi
Dostawa urządzeń zgodnie z tabelą poniżej	

Lp.	Typ sprzętu	Model	Producent	Nr seryjny
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

1. Niniejszy protokół stanowi podstawę do wystawienia faktury/rachunku
2. Wykonawca udziela Zamawiającemu licencji na oprogramowanie użyte do wykonania przedmiotu umowy. Wykonawca posiada dokumenty legalnego nabycia egzemplarzy programów wraz z podporządkowanymi temu nabyciu, udzielonymi przez producentów programów, licencjami.

Uwagi Wykonawcy	**Uwagi Zamawiającego**

…….. ……..

DATA i CZYTELNY podpis przedstawiciela Wykonawcy DATA i CZYTELNY podpis przedstawiciela Zamawiającego

Załącznik nr 2 tabela techniczna zamówienia do umowy z dnia …….. 2021r.

Załącznik nr 3 formularz cen jednostkowych do umowy z dnia ……. 2021r.

Zestawienie oferowanego sprzętu komputerowego (wraz z cenami jednostkowymi)

Lp.	**Nazwa**	**Producent/model/typ**	**Ilość**	Cena netto (szt.)	Cena brutto	Wartość brutto
1						
2						
3						
4						

Istotne warunki umowy (dotyczy części 2 przedmiotu zamówienia)

zawarta w Białymstoku ……. 2021 r. pomiędzy:

Polskim Radiem – Regionalną Rozgłośnią w Białymstoku „Radio Białystok" Spółką Akcyjną z siedzibą w Białymstoku (15-328) przy ul. Świerkowej 1, wpisaną do Krajowego Rejestru Sądowego w Sądzie Rejonowym w Białymstoku XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000037873, z kapitałem zakładowym 783 300,00 zł wpłaconym w całości, REGON: 050252837, NIP: 542-00-03-367, zwaną dalej "**Zamawiającym**", reprezentowaną przez:
Wojciecha Straszyńskiego – Prezesa zarządu
a
……

……

zwanym dalej „**Wykonawcą**" reprezentowanym przez:
…….

łącznie zwanymi "Stronami"

§ 1.

1. Przedmiotem Umowy jest dostawa na rzecz Zamawiającego oprogramowania zgodnie ze Szczegółowym Opisem Przedmiotu Zamówienia (Tabela techniczna zamówienia) stanowiącym załącznik nr 2 do Umowy. Wykonawca dostarczy do siedziby Zamawiającego oprogramowanie wraz z licencjami. Przedmiot Umowy zwany jest dalej również „oprogramowaniem" lub „przedmiotem zamówienia".
2. Wykonawca zapewni również usługę instalacji i skonfigurowania redundantnego rozwiązania systemu poczty oraz przeprowadzenia migracji skrzynek oraz poczty, folderów publicznych, grup dystrybucyjnych ze starego serwera na nowe rozwiązanie na zasadach określonych w załączniku nr 2.

§ 2.

1. Wykonawca oświadcza, że parametry techniczne i użytkowe oprogramowania są zgodne ze złożoną ofertą w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, znak: ZP 215.04.2021.
2. Wykonawca odpowiada za wady prawne dostarczonego oprogramowania.
3. Wykonawca oświadcza, że przedmiot Umowy jest wolny od jakichkolwiek wad prawnych oraz roszczeń osób trzecich.
4. Wykonawca dostarczy przedmiot Umowy na własny koszt, własnym staraniem i na własne ryzyko do siedziby Radia Białystok ul. Świerkowa 1 15-328 w godz. 9.00-15.00 w dniu roboczym.
5. Upoważniony przedstawiciel Zamawiającego sprawdzi zgodność dostarczonego oprogramowania w siedzibie Zamawiającego.
6. Do potwierdzenia wykonania przedmiotu Umowy niezbędne jest protokolarne przekazanie przez Wykonawcę przedmiotu Umowy i dokonanie przez Zamawiającego odbioru bez zastrzeżeń. Wzór protokołu odbioru stanowi Załącznik nr 1 do Umowy.
7. W przypadku niezgodności przedmiotu Umowy lub stwierdzenia innych wad podczas odbioru, Wykonawca zobowiązany jest niezwłocznie, nie przekraczając terminu, o którym mowa w §3 ust. 1, dostarczyć na własny koszt oprogramowanie wolne od wad i zgodny z przedmiotem Umowy.
8. Wykonawca odpowiada z tytułu rękojmi za wady na zasadach wynikających z Kodeksu cywilnego przez okres równy okresowi gwarancji.

§ 3.

1. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy, o którym mowa w §1 ust. 1, w terminie do …….. 2021 r.
2. Za termin realizacji przedmiotu Umowy przyjmuje się wskazaną, w podpisanym przez Strony bez zastrzeżeń protokole odbioru, datę wykonania bez wad całości przedmiotu Umowy, o którym mowa w §1 ust. 1.
3. Jeżeli termin na wykonanie zobowiązania kończy się w sobotę lub dzień ustawowo wolny od pracy przyjmuje się, że termin upływa następnego dnia roboczego.

§ 4.

1. Wynagrodzenie Wykonawcy z tytułu realizacji przedmiotu umowy wynosi: …….. zł brutto (słownie złotych: ……. ……), w tym VAT …….. zł (słownie złotych: ……..), netto …….. zł (słownie złotych: ……..).
2. Ceny jednostkowe brutto sprzętu zawiera formularz stanowiący Załącznik nr 3 do Umowy.
3. Wykonawcy przysługuje wynagrodzenie za przedmiot Umowy dostarczony i odebrany protokolarnie przez Zamawiającego bez zastrzeżeń.
4. Wynagrodzenie Wykonawcy, o którym mowa w ust. 1, jest ostateczne i obejmuje wszystkie koszty i opłaty towarzyszące wykonaniu Umowy, jakie mogą powstać w związku z jej realizacją, w tym koszty opłat pośrednich, celnych, podatek od towarów i usług (VAT), ubezpieczenie, koszt transportu, załadunku i rozładunku, koszty wymiany wadliwego przedmiotu zamówienia na pozbawiony wad, koszty odbioru i dostarczenia elementów podlegających wymianie gwarancyjnej, koszty serwisu gwarancyjnego, opłat licencyjnych oraz inne usługi/koszty związane z wykonaniem przedmiotu zamówienia, etc.

§ 5.

1. Należność za dostarczone oprogramowanie płatna będzie przelewem na rachunek bankowy Wykonawcy wskazany na „Białej liście" podatników VAT na stronie internetowej Ministerstwa Finansów w terminie do 14 dni kalendarzowych od dnia otrzymania prawidłowo wystawionej przez Wykonawcę faktury.
2. Za dzień zapłaty ustala się dzień wydania dyspozycji dokonania przelewu bankowi prowadzącemu rachunek Zamawiającego
3. Strony zobowiązują się do wzajemnego informowania o wszelkich zmianach danych, które mogą wpływać na wystawianie i obieg faktur oraz ich księgowanie i rozliczanie dla celów podatkowych, takich jak nazwa, adres, numer rachunku bankowego, NIP itp.
4. Podstawą do wystawienia faktury jest protokół odbioru podpisany przez Zamawiającego bez zastrzeżeń.
5. Wykonawca zobowiązany jest wystawiać na Zamawiającego faktury wynikające z realizacji Umowy i przekazać je Zamawiającemu, zgodnie z jego wyborem w formie papierowej lub elektronicznej:
   a) dla faktur w formie papierowej: faktura zostanie wystawiona na Zamawiającego, tj. Polskie Radio – Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A., ul. Świerkowa 1, 15-328 Białystok, NIP 542-00-03-367, i zaadresowana: Polskie Radio – Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A., ul. Świerkowa 1, 15-328 Białystok;
   b) dla faktur w formie elektronicznej: faktura zostanie wystawiona na Zamawiającego, tj.: Polskie Radio – Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A., ul. Świerkowa 1, 15-328 Białystok, NIP 542-00-03-367 i przekazana w formie elektronicznej z poczty elektronicznej Wykonawcy ..... na adres poczty elektronicznej Zamawiającego: sekretariat@radio.bialystok.pl
6. W przypadku przekazywania faktur w formie elektronicznej, zgodnie z ust. 5 pkt b), Wykonawca zobowiązuje się złożyć stosowane oświadczenie przed wystawieniem faktury.
7. Zmiana adresów poczty elektronicznej wskazanych w ust. 5 pkt b) wymaga złożenia pisemnego oświadczenia, przy czym oświadczenie o dokonaniu zmiany przez Wykonawcę powinno zostać przedłożone Zamawiającemu przed wysłaniem faktury.

8. Wysłanie faktury z innego, niż wskazany w ust. 5 pkt b), adresu poczty elektronicznej, bez uprzedniego złożenia powyższego oświadczenia, o którym mowa w ust. 7, zwalania Zamawiającego z odpowiedzialności w przypadku braku zapłaty lub opóźnienia w zapłacie należności wynikającej z danej faktury.
9. W przypadku opóźnienia w zapłacie kwoty wynikającej z faktury, w sytuacji innej niż wskazana w ust. 8, Wykonawca jest uprawniony do żądania zapłaty przez Zamawiającego odsetek stosownie do obowiązujących przepisów za każdy dzień opóźnienia.

§ 6.

1. Wykonawca zapłaci Zamawiającemu następujące kary umowne:
   1) w wysokości 10% kwoty brutto, o której mowa w § 4 ust. 1, gdy Zamawiający odstąpi od Umowy w całości lub w części z przyczyn leżących po stronie Wykonawcy, w szczególności z przyczyn wymienionych w § 7 ust. 1 pkt 1 - 5 oraz § 7 ust. 3 .
   2) w wysokości 0,5 % kwoty brutto, o której mowa w § 4 ust. 1 za każdy rozpoczęty dzień roboczy zwłoki w realizacji przedmiotu Umowy w terminie, o którym mowa w § 3 ust.1,
2. W przypadku odstąpienia przez Zamawiającego od części Umowy Wykonawcy przysługuje wynagrodzenie jedynie za prawidłowo wykonaną, potwierdzoną przez Zamawiającego część Umowy.
3. Jeżeli na skutek niewykonania lub nienależytego wykonania części lub całości przedmiotu Umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną bądź szkoda powstanie z innych przyczyn niż te, dla których zastrzeżono kary umowne, Zamawiającemu przysługuje prawo do dochodzenia odszkodowań uzupełniających na zasadach ogólnych Kodeksu cywilnego.
4. Zapłata kar umownych, o których mowa w ust. 1 pkt 2 nie zwalnia Wykonawcy od obowiązku wykonania Umowy.
5. Zamawiający ma prawo do potrącenia z wartości wynagrodzenia za wykonanie przedmiotu Umowy wartości naliczonych kar, a w przypadku niedokonania potrącenia kara umowna jest płatna w terminie do 14 dni kalendarzowych, od daty otrzymania przez Wykonawcę wezwania do jej zapłaty.
6. Kary umowne podlegają sumowaniu.

§ 7.

1. Zamawiający zastrzega sobie prawo odstąpienia od całości lub części niezrealizowanej Umowy ze skutkiem natychmiastowym (bez wyznaczania Wykonawcy dodatkowego terminu w tym zakresie) w następujących okolicznościach:
   1) w przypadku, gdy Wykonawca nie wykona przedmiotu Umowy w terminie, o którym mowa w § 3 ust. 1,
   2) w przypadku zwłoki Wykonawcy w wykonaniu innych zobowiązań objętych Umową, przekraczającej 7 dni kalendarzowych,
   3) niedostarczenia sprzętu fabrycznie nowego,
   4) innego rodzaju nienależytego wykonania lub niewykonania Umowy, czyniącego dalsze jej realizowanie bezprzedmiotowym,
   5) gdy otwarto likwidację majątku Wykonawcy,
   6) w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
2. Zamawiający może odstąpić od Umowy na podstawie ust. 1 pkt 1-5 w terminie 30 dni od dnia powzięcia przez Zamawiającego wiadomości o zaistnieniu przyczyny do odstąpienia.
3. Zamawiający może również odstąpić od Umowy w całości lub w części w innych sytuacjach przewidzianych w Kodeksie cywilnym.
4. Odstąpienie od Umowy wymaga formy pisemnej.

§ 8.

1. Wykonawca nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na rzecz osób trzecich bez pisemnej zgody Zamawiającego.

2. Zamawiający dopuszcza zmianę postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w zakresie:
   1) w przypadku wycofania z rynku lub braku dostępności na rynku zaoferowanego oprogramowania, dopuszcza się dostarczenie przez Wykonawcę innego oprogramowania o parametrach i funkcjonalnościach nie gorszych niż wynikające z oferty; warunki dostawy oraz warunki wykonywania świadczeń gwarancyjnych pozostają bez zmian; wynagrodzenie Wykonawcy nie może ulec zwiększeniu,
   2) innych zmian, w zakresie dopuszczonym art. 144 ustawy Pzp.
3. Zmiany wskazane w ust. 2 wymagają formy pisemnej w postaci aneksu, pod rygorem nieważności. W przypadku zmian wskazanych w ust. 2 pkt. 1 Wykonawca dodatkowo zobowiązany jest do przedstawienia Zamawiającemu informacji o proponowanej zmianie wraz z wyjaśnieniem przyczyn proponowanej zmiany i uprawdopodobnieniem zajścia przesłanek uprawniających do zmiany.

§ 9.

1. Wykonawca oświadcza i gwarantuje, że zawarcie Umowy przez Wykonawcę, jej wykonanie, oraz korzystanie z licencji przez Zamawiającego zgodnie z Umową, nie narusza praw własności intelektualnej producenta oprogramowania, ani jakichkolwiek innych osób trzecich, w tym praw autorskich lub patentów.
2. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z Umową, w szczególności zarzucających naruszenie praw własności intelektualnej, Wykonawca podejmie wszelkie działania mające na celu zażegnanie sporu i poniesie w związku z tym wszelkie koszty od chwili wystąpienia przez osobę trzecią z roszczeniem wobec Zamawiającego, w tym koszty procesu, zastępstwa procesowego oraz odszkodowań. W szczególności, w razie wytoczenia przeciwko Zamawiającemu powództwa z tytułu naruszenia praw własności intelektualnej, Wykonawca wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie Zamawiającego.
3. Jeżeli wskutek orzeczenia sądu Zamawiający nie będzie mógł korzystać z przedmiotu Umowy, Wykonawca, na swój koszt i według własnego wyboru, uzyska dla Zamawiającego prawa do przedmiotu Umowy lub dokona wymiany na przedmiot nie naruszający praw. W przypadku jeżeli powyższe okaże się niemożliwe, Wykonawca będzie zobowiązany do zwrotu Zamawiającemu zapłaconego przez Zamawiającego wynagrodzenia.

§ 10.

1. Wykonawca i Zamawiający zobowiązują się do zapewnienia prawidłowego przetwarzania, udostępnionych przez drugą stronę, danych osobowych poprzez stosowanie odpowiednich organizacyjnych i technicznych środków ochrony tych danych, gwarantujących ochronę praw osób, których te dane dotyczą, zgodnie z przepisami i wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO), zapisami Ustawy z dnia 10.05.2018 r. o ochronie danych osobowych z późniejszymi zmianami (Dz. U. z 2018 r. poz.1000) lub innymi przepisami prawa polskiego, a w szczególności zobowiązują się jako podmiot przetwarzający do przestrzegania obowiązków wynikających z art. 28 i nast. wspomnianego rozporządzenia.
2. Na podstawie niniejszej umowy Wykonawca powierza Zamawiającemu przetwarzanie (w szczególności zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, wykorzystywanie, przesyłanie, usuwanie, niszczenie) następujących kategorii danych osobowych: imię i nazwisko oraz funkcja lub stanowisko osób reprezentujących Wykonawcę, imię i nazwisko osób wykonujących prace w ramach realizacji przedmiotu umowy, jeżeli przekazanie tych danych będzie konieczne w związku z realizacją przedmiotu umowy oraz osób wskazanych do kontaktu w związku z realizacją przedmiotu umowy przez okres trwania niniejszej umowy, a także adres e-mail lub telefon osób wskazanych do kontaktu. Charakter przetwarzania danych dotyczy przetwarzania danych osobowych w formie papierowej i przy wykorzystaniu systemów informatycznych.

3. Na podstawie niniejszej umowy Zamawiający powierza Wykonawcy przetwarzanie (w szczególności zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, wykorzystywanie, przesyłanie, usuwanie, niszczenie) następujących kategorii danych osobowych: imię i nazwisko oraz funkcja lub stanowisko osób reprezentujących Zamawiającego oraz, imię i nazwisko osób wskazanych do kontaktu w związku z realizacją przedmiotu umowy, przez okres trwania niniejszej umowy, a także adres e-mail lub telefon osób wskazanych do kontaktu. Charakter przetwarzania danych dotyczy przetwarzania danych osobowych w formie papierowej i przy wykorzystaniu systemów informatycznych.
4. Wykonawca zobowiązuje się do zapoznania swoich współpracowników (niezależnie od podstawy prawnej współpracy) oraz podmiotów, za pośrednictwem, których realizować będzie niniejszą umowę z zasadami i procedurami związanymi z ochroną danych osobowych, w zakresie, w jakim te zasady i procedury będą miały wpływ na realizację umowy.
5. Strona przetwarzająca powierzone dane, przetwarza je zgodnie z poleceniem drugiej strony (administratora danych) i jest uprawniona do upoważnienia poszczególnych osób do przetwarzania ich w takim zakresie. Jednocześnie podmiot przetwarzający zapewni, by osoby upoważnione do przetwarzania danych osobowych zobowiązane były do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
6. Strona, której powierzono przetwarzanie danych po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki zgłasza je drugiej stronie (administratorowi), nie później niż w ciągu 24 godzin od stwierdzenia naruszenia poprzez: telefoniczny kontakt Zamawiającego 85 745 62 20 lub mailem na adres sekretariat@radio.bialystok.pl, telefoniczny kontakt Wykonawcy ……. lub mailem na adres ……...
7. Wykonawca i Zamawiający oświadczają, że dane osobowe, o których mowa w ust. 2-3, zostaną wykorzystane wyłącznie w celu realizacji przedmiotu umowy.
8. Wykonawca i Zamawiający zobowiązują się do przekazania lub trwałego zniszczenia we własnym zakresie (zgodnie z decyzją administratora), niezwłocznie po zakończeniu realizacji Umowy, ewentualnych dokumentów, ich kopii lub nośników zawierających dane osobowe, o których mowa w ust. 2-3, przy uwzględnieniu terminów obowiązkowego przechowywania dokumentów wynikających z obowiązujących przepisów.
9. Odpowiednio każda ze stron jako administrator zobowiązuje się i oświadcza, że będzie wypełniała obowiązki informacyjne przewidziane w art. 13 lub 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskała w celu realizacji przedmiotu umowy, a druga strona zobowiązuje się do współpracy w zakresie wykonania tego obowiązku.

§ 11.

Obowiązek informacyjny w związku z przetwarzaniem danych osobowych:

1. Administratorem danych osobowych jest Radio Białystok S.A. (dalej: „ADMINISTRATOR”), z siedzibą: ul. Świerkowa 1, 15-328 Białystok. Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: ul. Świerkowa 1, 15-328 Białystok lub drogą e-mailową pod adresem: iodo@radio.bialystok.pl.
2. Administrator wyznaczył Inspektora Ochrony Danych – Andrzeja Rybus-Tołłoczko, z którym można się skontaktować pod adresem mailowym: iodo@radio.bialystok.pl.
3. Pani/Pana dane osobowe są przetwarzane na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.
4. Przetwarzanie danych odbywa się w związku z:
   a) realizacją umowy na zlecone zamówienie publiczne – art. 6 ust. 1 lit. b RODO;
   b) rozliczeniem umowy – art. 6 ust. 1 lit. c RODO;

c) realizacją zadania publicznego w ramach zamówienia publicznego – art. 6 ust. 1 lit. e RODO;
d) dochodzeniem i obroną roszczeń – art. 6 ust. 1 lit. f RODO,

5. Dane osobowe nie pochodzą od stron trzecich.
6. Administrator nie zamierza przekazywać danych do państwa trzeciego lub organizacji międzynarodowej.
7. Administrator nie zamierza przekazywać danych osobowych, a jeżeli musiałoby to nastąpić, to tylko na podstawie przepisów prawa, w tym do Urzędu Zamówień Publicznych, Organów Kontrolnych lub umowy powierzenia przetwarzania danych osobowych, w tym do dostawców usług teleinformatycznych, biur rachunkowych świadczących usługi na rzecz Administratora.
8. Dane będą przetwarzane przez okres 10 lat od początku roku następującego po roku, w którym nastąpiła realizacja zamówienia.
9. Osoba, której dane dotyczą ma prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
10. Skargę na działania Administratora można wnieść do Prezesa Urzędu Ochrony Danych Osobowych.
11. Podanie danych osobowych jest wymogiem prawa. Ich nie podanie spowoduje brak możliwości zawarcia umowy na realizację zamówienia publicznego, a co za tym idzie odstąpienie od jego realizacji.
12. Administrator nie przewiduje zautomatyzowanego podejmowania decyzji.

§ 12.

1. Na potrzeby niniejszej umowy przez dni robocze strony rozumieją dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
2. We wszystkich sprawach nieuregulowanych w niniejszej Umowie zastosowanie mają przepisy prawa polskiego, w szczególności przepisy:
   a) ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny,
   b) ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.
3. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Strony będą dążyły do polubownego rozstrzygania wszystkich sporów powstałych w związku z wykonywaniem niniejszej Umowy. W przypadku nieosiągnięcia porozumienia w drodze negocjacji, wszelkie spory rozstrzygane będą przez sąd miejscowo właściwy dla siedziby Zamawiającego.
5. Osoby wyznaczone do uzgodnień i koordynacji przedmiotu niniejszej Umowy:
   1) ze strony Zamawiającego – Jarosław Dobrowolski
   2) ze strony Wykonawcy – ……
6. Osobami upoważnionymi do podpisania protokołów odbioru:
   – ze strony Zamawiającego są: Jarosław Dobrowolski lub inne osoby upoważnione przez Zamawiającego,
   – ze strony Wykonawcy jest: ……
7. Zmiana osób, o których mowa w ust. 5 lub 6 może nastąpić po poinformowaniu drugiej strony i nie wymaga sporządzenia aneksu do Umowy.
8. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Załączniki:
Załącznik nr 1 – Wzór protokołu odbioru
Załącznik nr 2 – Tabela techniczna zamówienia
Załącznik nr 3 – Formularz cen jednostkowych

…… ……

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 protokół odbioru do umowy z dnia …….. 2021r.

PROTOKÓŁ ODBIORU

dotyczący realizacji postanowień umowy z dnia ……. 2021 do postępowania nr ZP.215.04.2021 na usługę dostawy oprogramowania

Wykonawca	**Zleceniodawca**
	Polskie Radio - Regionalna Rozgłośnia w Białymstoku „Radio Białystok" S.A. 15-328 Białystok ul. Świerkowa 1 NIP 542-00-03-367

Opis	Uwagi
Dostawa oprogramowania zgodnie z tabelą poniżej	

Lp.	Typ oprogramowania	Nazwa	Producent	Nr seryjny
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

1. Niniejszy protokół stanowi podstawę do wystawienia faktury/rachunku
2. Wykonawca udziela Zamawiającemu licencji na oprogramowanie użyte do wykonania przedmiotu umowy. Wykonawca posiada dokumenty legalnego nabycia egzemplarzy programów wraz z podporządkowanymi temu nabyciu, udzielonymi przez producentów programów, licencjami.

Uwagi Wykonawcy	**Uwagi Zamawiającego**

....

DATA i CZYTELNY podpis przedstawiciela Wykonawcy DATA i CZYTELNY podpis przedstawiciela Zamawiającego

Załącznik nr 2 tabela techniczna zamówienia do umowy z dnia …….. 2021r.

Załącznik nr 3 formularz cen jednostkowych do umowy z dnia ……. 2021r.

Zestawienie oferowanego oprogramowania (wraz z cenami jednostkowymi)

Lp.	**Nazwa**	**Producent/model/typ**	**Ilość**	Cena netto (szt.)	Cena brutto	Wartość brutto
1						
2						
3						
4						

Załącznik Nr 5 do SWZ **Znak sprawy ZP.215.04.2021**

Klauzula informacyjna RODO

W związku z udziałem w postępowaniu o udzielenie zamówienia publicznego informujemy:

1. Administratorem danych osobowych jest Radio Białystok S.A. (dalej: „ADMINISTRATOR"), z siedzibą: ul. Świerkowa 1, 15-328 Białystok. Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: ul. Świerkowa 1, 15-328 Białystok lub drogą e-mailową pod adresem: iodo@radio.bialystok.pl.
2. Administrator wyznaczył Inspektora Ochrony Danych - Andrzeja Rybus-Tołłoczko, z którym można się skontaktować pod adresem mailowym: iodo@radio.bialystok.pl.
3. Dane osobowe są przetwarzane na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.
4. Przetwarzanie danych osobowych odbywa się w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego – art. 6 ust. 1 lit. c, e RODO - dane osobowe będą przetwarzane przez Administratora do 5 lat od dnia zakończenia postępowania o udzielenie zamówienia, zgodnie z przepisami prawa
5. Dane osobowe nie pochodzą od stron trzecich.
6. Administrator nie zamierza przekazywać danych do państwa trzeciego lub organizacji międzynarodowej.
7. Administrator będzie przekazywał dane osobowe innym podmiotom, tylko na podstawie przepisów prawa, w tym w szczególności do: Urzędu Zamówień Publicznych, organów kontrolnych, a także na podstawie zawartych umów powierzenia przetwarzania danych osobowych, w tym do dostawców usług teleinformatycznych.
8. Dane osobowe będą przetwarzane przez Administratora do 5 lat od dnia zakończenia postępowania o udzielenie zamówienia, zgodnie z przepisami prawa.
9. Osoba, której dane dotyczą ma prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
10. Skargę nas działania Administratora można wnieść do Prezesa Urzędu Ochrony Danych Osobowych.
11. Podanie danych osobowych jest wymogiem udziału w postępowaniu o udzielenie zamówienia. Ich niepodanie spowoduje brak możliwości udziału w postępowaniu.
12. Administrator nie przewiduje zautomatyzowanego podejmowania decyzji.

Zapoznanie się z informacją o przetwarzaniu danych:

Ja, ……..…… zapoznałem/am się z obowiązkiem informacyjnym.

…… ……
/data/ /podpis/

Załącznik Nr 6 do SWZ **Znak sprawy ZP.215.04.2021**

.....
Pieczęć Wykonawcy

Wykaz podwykonawców i zakres zamówienia przez nich wykonywanego

Oświadczamy, że przy realizacji zamówienia publicznego pod nazwą: dostawa sprzętu komputerowego i oprogramowania do Polskiego Radia Białystok S.A. będą uczestniczyć następujący podwykonawcy:

Lp.	Nazwa i adres przewidywanego podwykonawcy	Zakres powierzonego zamówienia
1.		
2.		
3.		

…….
*(*Podpis wykonawcy lub upełnomocnionego przedstawiciela wykonawcy*)*