SPECYFIKACJA WARUNKÓW ZAMÓWIENIA
ZAMÓWIENIE KLASYCZNE

CNT.371.037.2021

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie”

Przetarg nieograniczony - art. 132 i nast. Pzp
Zamówienie o wartości równiej lub powyżej progów unijnych

Zamówienie prowadzone jest w oparciu o przepisy ustawy z dnia 11 września 2019 r.
Prawo zamówień publicznych (Dz. U. 2021 r. poz. 1129 ze zm.)

Zatwierdzenie:

Kierownik projektu: …….

Kierownik jednostki: ……

Kierownik Zamawiającego: ……

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

1. Adres: ul. Dewajtis 5, 01-815 Warszawa
2. Adres strony internetowej: www.uksw.edu.pl
3. REGON: 000001956
4. NIP: 525-00-12-946

II. STRONA INTERNETOWA PROWADZONEGO POSTĘPOWANIA

1. Komunikacja w postępowaniu o udzielenie zamówienia odbywa się przy użyciu środków komunikacji elektronicznej. Szczegółowy opis komunikacji w postępowaniu znajduje się w dalszej części SWZ, w szczególności w rozdziale XVII SWZ.
2. Adres platformy zakupowej: **https://platformazakupowa.pl/pn/uksw.**
3. Na Platformie zakupowej Zamawiający udostępnia wszystkie podlegające obowiązkowi publikacji na stronie postępowania informacje.

III. TRYB UDZIELENIA ZAMÓWIENIA

1. Tryb udzielenia zamówienia – przetarg nieograniczony.
2. Na podstawie art. 139 ustawy Pzp (tzw. procedura odwrócona) Zamawiający najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej wykonawcy, którego oferta została najwyżej oceniona, w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu. Opis procedury został zawarty w art. 139 ustawy Pzp.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych.**
2. Przedmiot zamówienia opisują poniższe kody CPV
   38500000 – 0 Aparatura kontrolna i badawcza
   48820000-2 Serwery
   32420000-3 Urządzenia sieciowe
3. Szczegółowo przedmiot zamówienia określono **w załączniku nr 5 do SWZ.**
4. Zamawiający informuje, że tam, gdzie w SWZ opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, Zamawiający dopuszcza rozwiązania równoważne do opisanych w opisie przedmiotu zamówienia pod warunkiem, że będą one spełniały określone w opisie przedmiotu zamówienia kryteria stosowane w celu oceny równoważności. Tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 Pzp Zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą słowa „**lub równoważne**”.
5. Zamawiający wskazuje, **że obowiązek zgłoszenia w ofercie rozwiązań równoważnych w stosunku do opisanych w opisie przedmiotu zamówienia i wykazania równoważności leży po stronie wykonawcy**.
6. W przypadku gdy wymagania w opisie przedmiotu zamówienia odnoszą się do znaku towarowego, patentu lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje konkretne produkty lub usługi Zamawiający wymaga, aby wykonawca w przypadku zaoferowania rozwiązań równoważnych, przedstawił już w jego ofercie dowód równoważności potwierdzający spełnienie kryteriów, które Zamawiający stosuje w celu oceny równoważności (Wyrok TSUE C-14/17 z dnia 2018-07-12) np. karty katalogowe produktów. W przypadku gdy wymagania w opisie przedmiotu zamówienia odnoszą się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 Pzp, Zamawiający wymaga, aby wykonawca przedstawił już w jego ofercie dowody równoważności w sposób określony w art. 101 ust. 5 i 6 Pzp.
7. Zamawiający żąda aby wykonawca, który zaproponował rozwiązania równoważne, o których mowa w art. 101 ust. 4 Pzp przedstawił dowody równoważności, o których mowa w art. 101 ust. 5 i 6 Pzp w szczególności określone tam przedmiotowe środki dowodowe. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wzywa do ich złożenia lub uzupełnienia w wyznaczonym terminie.

V. INFORMACJA O PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH

Zamawiający nie żąda od wykonawcy złożenia wraz z ofertą przedmiotowych środków dowodowych, z zastrzeżeniem Części IV SWZ.

VI. DOPUSZCZENIE SKŁADANIA OFERT CZĘŚCIOWYCH

1. Przedmiot zamówienia nie został podzielony na części.

2. Z uwagi na przedmiot zamówienia jego podział na części nie ma uzasadnienia ekonomicznego i praktycznego oraz uniemożliwiłby uzyskanie niezbędnych i potrzebnych zamawiającemu funkcjonalności. Warunki realizacji w tym: wysokość zaangażowanych środków finansowych, organizacyjnych, doświadczenia – nie wykluczają z udziału w przedmiotowym postępowaniu małych i średnich przedsiębiorstw.

VII. WYMAGANIA W ZAKRESIE ZATRUDNIENIA NA PODSTAWIE STOSUNKU PRACY

Niniejsze zamówienie jest dostawą. Zamawiający nie określa wymagań zatrudnienia na podstawie stosunku pracy.

VIII. TERMIN WYKONANIA ZAMÓWIENIA

Zamawiający wymaga wykonania zamówienia w terminie **120 dni** od dnia zawarcia umowy w sprawie zamówienia publicznego.

IX. PODSTAWY WYKLUCZENIA OBLIGATORYNE (ART. 108 PZP)

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:
   1) nie podlegają wykluczeniu;
   2) spełniają warunki udziału w postępowaniu, o ile zostały określone w niniejszej SWZ.
2. Z postępowania o udzielenie zamówienia Zamawiający wykluczy wykonawcę:
   1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

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

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów złożyli odrębne oferty, oferty częściowe, chyba że wykażą, że przygotowali te oferty niezależnie od siebie;
6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny

sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

X. PODSTAWY WYKLUCZENIA FAKULTATYWNE (ART. 109 PZP)

Zamawiający nie przewiduje wykluczenia Wykonawcy na podstawie art. 109 Pzp.

XI. SAMOOCZYSZCZENIE

1. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2, 5 Pzp, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:
   1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
   2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
   3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
      a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
      b) zreorganizował personel,
      c) wdrożył system sprawozdawczości i kontroli,
      d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
      e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.
2. Zamawiający oceni czy podjęte przez wykonawcę czynności, o których mowa w ust. 2, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności, o których mowa w ust. 2, nie są wystarczające do wykazania jego rzetelności, Zamawiający wykluczy wykonawcę.

XII. OKRESY WYKLUCZENIA

Wykluczenie wykonawcy następuje:

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

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

   – na okres 3 lat od dnia uprawomocnienia się odpowiednio wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, wydania ostatecznej decyzji lub zaistnienia zdarzenia będącego podstawą wykluczenia, chyba że w wyroku lub decyzji został określony inny okres wykluczenia;
3) w przypadku, o którym mowa w art. 108 ust. 1 pkt 4 Pzp, na okres, na jaki został prawomocnie orzeczony zakaz ubiegania się o zamówienia publiczne;
4) w przypadkach, o których mowa w art. 108 ust. 1 pkt 5 Pzp, na okres 3 lat od zaistnienia zdarzenia będącego podstawą wykluczenia;
7) w przypadkach, o których mowa w art. 108 ust. 1 pkt 6 Pzp, w postępowaniu o udzielenie zamówienia, w którym zaistniało zdarzenie będące podstawą wykluczenia.

XIII. INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU O UDZIELENIE ZAMÓWIENIA

1. Zamawiający określa poniższe warunki udziału w postępowaniu dotyczące:

1) zdolności do występowania w obrocie gospodarczym:
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie.
2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie.
3) sytuacji ekonomicznej lub finansowej:
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie.
4) zdolności technicznej lub zawodowej:
Zamawiający uzna, że Wykonawca, spełnia warunek jeżeli w okresie ostatnich 3 lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie), wykonał lub wykonuje w ramach jednej umowy co najmniej jedną dostawę sprzętu komputerowego o wartości nie mniejszej niż 1 000 000 zł brutto.

2. Zamawiający w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia wymaga, aby każdy z w/w niniejszym punkcie warunków potwierdził co najmniej jeden z tych wykonawców.
3. Warunek dotyczący uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej (jeżeli jest wymagany) jest spełniony, jeżeli co najmniej jeden z wykonawców wspólnie ubiegających się o udzielenie zamówienia posiada uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej i zrealizuje roboty budowlane, dostawy lub usługi, do których realizacji te uprawnienia są wymagane.
4. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia (jeżeli jest wymagany), wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
5. W przypadkach, o którym mowa w ust. 3-4, wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które

roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy. Formularz oświadczenia **stanowi załącznik nr 4 do SWZ.**

XIV. POLEGANIE NA ZDOLNOŚCIACH LUB SYTUACJI PODMIOTÓW UDOSTĘPNIAJĄCYCH ZASOBY

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia **stanowi załącznik nr 3 do SWZ** lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust. 3, powinno potwierdzać, że stosunek łączący wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa, w szczególności:
   1) zakres dostępnych wykonawcy zasobów podmiotu udostępniającego zasoby;
   2) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
5. Zamawiający oceni, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu określonych w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.
6. Podmiot, który zobowiązał się do udostępnienia zasobów, **odpowiada solidarnie z wykonawcą**, który polega na jego sytuacji finansowej lub ekonomicznej, za szkodę poniesioną przez zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów podmiot ten nie ponosi winy.
7. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, zamawiający żąda, aby wykonawca w terminie określonym przez zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.

8. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

XV. WYKONAWCY WSPÓLNIE UBIEGAJĄCY SIĘ O UDZIELENIE ZAMÓWIENIA

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
2. W przypadku, o którym mowa w ust. 1, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
3. Jeżeli została wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający **będzie żądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych wykonawców**.
4. Zamawiający nie zastrzega obowiązku osobistego wykonania przez poszczególnych wykonawców wspólnie ubiegających się o udzielenie zamówienia kluczowych zadań dotyczących prac związanych z rozmieszczeniem i instalacją, w ramach zamówienia na dostawy.

XVI. OŚWIADCZENIE WSTĘPNE (JEDZ) ORAZ PODMIOTOWE ŚRODKI DOWODOWE

1. Do oferty wykonawca dołącza oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu, w zakresie wskazanym przez Zamawiającego, w **załączniku nr 2 do SWZ**.
2. Oświadczenie, o którym mowa w ust. 1, składa się na formularzu jednolitego europejskiego dokumentu zamówienia, sporządzonym zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu Wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16) (**JEDZ**/ESPD).
3. Oświadczenie, o którym mowa w ust. 1, stanowi dowód potwierdzający brak podstaw wykluczenia, spełnianie warunków udziału w postępowaniu, odpowiednio na dzień składania ofert, tymczasowo zastępujący wymagane przez zamawiającego podmiotowe środki dowodowe.
4. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w ust. 1, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
5. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w ust. 1, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby.

6. **Zamawiający od wykonawcy, który zostanie oceniony najwyżej będzie żądał poniższych podmiotowych środków dowodowych na potwierdzenie braku podstaw wykluczenia**
   1) informacji z Krajowego Rejestru Karnego w zakresie:
      a) **art. 108 ust. 1 pkt 1 i 2 Pzp**,
      b) **art. 108 ust. 1 pkt 4 Pzp**, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne **tytułem środka karnego**,

      - sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;
   2) oświadczenia wykonawcy, w zakresie **art. 108 ust. 1 pkt 5 Pzp**, **o braku przynależności do tej samej grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu , albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej; (**Załącznik nr 8 do SWZ**)
   3) oświadczenia wykonawcy (**Załącznik nr 7 do SWZ**) o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 Pzp (JEDZ), w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:
      a) art. 108 ust. 1 pkt 3 Pzp,
      b) art. 108 ust. 1 pkt 4 Pzp, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
      c) art. 108 ust. 1 pkt 5 Pzp, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
      d) art. 108 ust. 1 pkt 6 Pzp.

   Na wezwanie Zamawiającego powyższe oświadczenia składa wykonawca, wykonawcy wspólnie ubiegający się o zamówienie,
7. Jeżeli wykonawca (wykonawca wspólnie ubiegający się o zamówienie, odpowiednio podmiot udostępniający zasoby) ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast:
   1) informacji z Krajowego Rejestru Karnego, o której mowa w ust. 6 pkt 1 - składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w ust. 6 pkt 1;
8. Dokument, o którym mowa w ust. 7 pkt 1, powinien być wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem.
9. Jeżeli w kraju, w którym wykonawca (wykonawca wspólnie ubiegający się o zamówienie, odpowiednio podmiot udostępniający zasoby) ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 7, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4 Pzp, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy (wykonawcy wspólnie ubiegający się o zamówienie, odpowiednio podmiotu udostępniającego zasoby), ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed

organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy. Przepis ust. 8 stosuje się.

10. Zamawiający **żąda** poniższych podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu:

wykaz dostaw, *a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy lub usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostaw zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy;* (**Załącznik nr 9 do SWZ**)

11. Zamawiający wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni od dnia wezwania, podmiotowych środków dowodowych, w zakresie wskazanym w ust. 6 -10, aktualnych na dzień ich złożenia.
12. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:

1) 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, o ile wykonawca wskazał w jednolitym dokumencie (JEDZ) dane umożliwiające dostęp do tych środków;
2) podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1 Pzp.

13. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, określonych w ust. 6-10, aktualnych na dzień ich złożenia.
14. 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.

XVII. INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI, ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między zamawiającym a wykonawcą, z uwzględnieniem wyjątków określonych w Pzp, odbywa się przy użyciu środków komunikacji elektronicznej.
2. *W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a wykonawcami odbywa się* ***za pośrednictwem platformy zakupowej.***
   2.1. Adres platformy zakupowej: **https://platformazakupowa.pl/pn/uksw.**
3. Komunikacja ustna lub za pośrednictwem e-mail dopuszczalna jest wyłącznie w odniesieniu do informacji, które nie są istotne, w szczególności nie dotyczą treści ogłoszenia o zamówieniu lub treści dokumentów zamówienia, o ile jej treść zostanie udokumentowana.
   3.1. Osoba upoważniona: ***Piotr Kmieć***
   3.2. *adres e-mail:* ***p.kmiec@uksw.edu.pl***
   3.3. ***tel.: 509 687 445***

4. **Forma dokumentów elektronicznych:**
   4.1. Ofertę, oświadczenia, o których mowa w art. 125 ust. 1 Pzp (określone w części XVI ust. 1 -4 SWZ), podmiotowe środki dowodowe, o których mowa w części XVI ust. 6 SWZ, w tym oświadczenie wykonawców wspólnie ubiegających się o zamówienie, o którym mowa w art. 117 ust. 4 Pzp (określone w części XVI SWZ), zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, niewystawione przez upoważnione podmioty oraz pełnomocnictwo, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568, 695, 1517 i 2320).
   4.2. Ofertę, oświadczenia, o których mowa w art. 125 ust. 1 Pzp, wykonawca składa pod rygorem nieważności, **w formie elektronicznej (podpisanej kwalifikowanym podpisem elektronicznym)**.
   4.3. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania", zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami", jako dokument elektroniczny, wykonawca przekazuje ten dokument.
   4.4. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, wykonawca przekazuje cyfrowe odwzorowanie tego dokumentu

opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.

4.5. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w ust. 4.4, dokonuje w przypadku:

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

2) przedmiotowych środków dowodowych - odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;

3) pełnomocnictwa – mocodawca;

4) innych dokumentów - odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.

4.6. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej może dokonać również notariusz.

4.7. 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.

4.8. Informacje, oświadczenia lub dokumenty, inne niż określone w ust. 4.2, przekazywane w postępowaniu sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej.

4.9. Podmiotowe środki dowodowe, w tym oświadczenie wykonawców wspólnie ubiegających się o zamówienie, o którym mowa w art. 117 ust. 4 Pzp, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.

4.10. Dokumenty elektroniczne w postępowaniu przekazywane przez wykonawcę muszą spełniać wymagania określone w § 10 ust. 1 Rozporządzenia 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. 2020 r. 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).

4.11. Użycie środków komunikacji elektronicznej służących do odbioru dokumentów elektronicznych jest uzależnione od podania przez wykonawcę danych umożliwiających jednoznaczną identyfikację użytkownika, a także akceptacji przez wykonawcę zasad korzystania ze środków komunikacji elektronicznej udostępnianych przez Zamawiającego.

4.12. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.

4.13. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku kwalifikowanym podpisem elektronicznym.

5. **<u>Opis sposobu przygotowania ofert oraz dokumentów wymaganych przez zamawiającego w SWZ</u>**

5.1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać opatrzone **elektronicznym kwalifikowanym podpisem**.

5.2. W procesie składania oferty, w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu.

5.3. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.

5.4. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej przez opatrzenie dokumentu kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnioną/upoważnione.

5.5. **Oferta powinna być:**

5.5.1. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem **Platformy Zakupowej**

5.5.2. opatrzona kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnioną/upoważnione.

5.6. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".

5.7. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.

5.8. Zgodnie z art. 18 ust. 3 Pzp, nie ujawnia się informacji **stanowiących tajemnicę przedsiębiorstwa**, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.

5.9. Wykonawca, za pośrednictwem Platformy Zakupowej może przed upływem terminu do składania wycofać ofertę. Sposób dokonywania wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: **https://platformazakupowa.pl/strona/45-instrukcje.**

5.10. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, Zgodnie z definicją dokumentu elektronicznego z art. 3 ustęp 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.

5.11. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

6. **Sposób oraz termin składania ofert**

6.1. Wykonawca składa ofertę za pośrednictwem Platformy dostępnej pod adresem: **https://platformazakupowa.pl/pn/uksw** w nieprzekraczalnym terminie (do dnia i godziny) określonym w części XXII pkt 1 SWZ. O terminie złożenia oferty decyduje czas pełnego przeprocesowania transakcji na Platformie.

6.2. Wykonawca składa ofertę w konkretnym postępowaniu w sprawie udzielenia zamówienia publicznego na stronie postępowania w miejscu oznaczonym jako „Formularz" służący do złożenia ofert, poprzez załączenie dokumentów (załączników) określonych w niniejszej SWZ i podpisanych kwalifikowanym podpisem elektronicznym poprzez wybranie polecenia „dołącz plik" i wybranie docelowego pliku, który ma zostać zamieszczony. W pkt. 1 Formularza Wykonawca załącza pliki jawne, natomiast w pkt. 2 Formularza Wykonawca załącza pliki stanowiące tajemnicę przedsiębiorstwa (o ile składa dane objęte tajemnicą przedsiębiorstwa).

6.3. Po wypełnieniu Formularza składania oferty i załadowaniu wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania".

6.4. Następnie należy kliknąć przycisk „Złóż ofertę", aby zakończyć etap składania oferty.

6.5. System zaszyfruje ofertę Wykonawcy, tak by ta była niedostępna dla Zamawiającego do terminu otwarcia ofert.

6.6. Ostatnim krokiem złożenia oferty jest wyświetlenie się komunikatu i przesłanie wiadomości
e-mail z platformazakupowa.pl z informacją na temat złożonej oferty.

6.7. Plik załączony przez Wykonawcę na Platformie i zapisany jest zaszyfrowany. Dlatego też dokumenty złożone na Platformie nie są widoczne do momentu odszyfrowania przez Zamawiającego, który następuje po terminie składania ofert.

6.8. Z uwagi na to, że dokumenty przesłane poprzez Formularz do składania ofert są zaszyfrowane nie można ich edytować. Przez zmianę oferty rozumie się złożenie nowej oferty i wycofanie poprzedniej, jednak należy to zrobić przed upływem terminu

zakończenia składania ofert w postępowaniu.

6.9. Złożenie nowej oferty i wycofanie poprzedniej oferty przed upływem terminu zakończenia składania ofert w postępowaniu powoduje wycofanie oferty poprzednio złożonej.

6.10. Jeśli Wykonawca składający ofertę jest zautoryzowany (zalogowany), to wycofanie oferty następuje od razu po złożeniu nowej oferty.

6.11. Jeżeli oferta składana jest przez niezautoryzowanego Wykonawcę (niezalogowanego lub nieposiadającego konta) to wycofanie oferty musi być przez niego potwierdzone w następujący sposób:

6.11.1. przez kliknięcie w link wysłany w wiadomości e-mail, który musi być zgodny z adresem e-mail podanym podczas pierwotnego składania oferty, potwierdzeniem wycofania oferty jest data potwierdzenia akcji przez kliknięcie w przycisk „Wycofaj ofertę".

6.11.2. poprzez zalogowanie i kliknięcie w przycisk „Potwierdź ofertę".

6.12. Wycofanie oferty możliwe jest do zakończenia terminu składania ofert.

6.13. Wycofanie złożonej oferty powoduje, że Zamawiający nie będzie miał możliwości zapoznania się z nią po upływie terminu zakończenia składania ofert w postępowaniu.

6.14. Jeżeli Wykonawca złoży ofertę po terminie na składanie ofert poprzez kliknięcie przycisku „Odblokuj formularz", po złożeniu oferty po terminie Wykonawca otrzyma automatyczny komunikat dotyczący tego, że oferta została złożona po terminie.

6.15. Wykonawca po upływie terminu na składanie ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty (załączników).

7. **<u>Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń lub dokumentów,</u>**

7.1. Postępowanie prowadzone jest w języku polskim przy użyciu środków komunikacji elektronicznej za pośrednictwem Platformy Zakupowej (w niniejszej SWZ nazywanej również jako „**Platforma**" lub „**Platforma Zakupowa**") dostępnej pod adresem: **<u>https://platformazakupowa.pl/pn/uksw</u>**

7.2. Komunikacja między zamawiającym a wykonawcami w zakresie:

7.2.1. przesyłania Zamawiającemu pytań do treści SWZ;

7.2.2. przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;

7.2.3. przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;

7.2.4. przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych

podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;

7.2.5. przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dot. treści przedmiotowych środków dowodowych;

7.2.6. przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;

7.2.7. przesyłania wniosków, informacji, oświadczeń Wykonawcy;

7.2.8. przesyłania odwołania

7.2.9. inne, z wyłączeniem oferty

odbywa się za pośrednictwem Platformy i formularza „Wyślij wiadomość do zamawiającego".

7.3. Komunikacja między zamawiającym a wykonawcami **w zakresie przesyłania oferty** odbywa się za pośrednictwem Platformy i **formularza do złożenia oferty**. Szczegóły opisane w punkcie 7 poniżej.

7.4. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem Platformy poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

7.5. Zamawiający będzie przekazywał wykonawcom za pośrednictwem Platformy informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert. Zamawiający będzie zamieszczał dokumenty na Platformie w sekcji "Komunikaty".

7.6. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana za pośrednictwem Platformy do konkretnego wykonawcy.

7.7. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na Platformie przesłanych przez Zamawiającego, gdyż

system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.

7.8. Zamawiający, określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na Platformie:

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

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

7.8.3. zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10.0,

7.8.4. włączona obsługa JavaScript,

7.8.5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików pdf.

7.8.6. Szyfrowanie na Platformie odbywa się za pomocą protokołu TLS 1.3

7.8.7. Oznaczenie czasu odbioru danych przez Platformę stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

7.9. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:

7.9.1. akceptuje warunki korzystania z Platformy określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący, zapoznał i stosuje się do Instrukcji składania ofert/wniosków na Platformie.

7.9.2. bezpłatnie rejestrując się lub logując, w przypadku posiadania konta na Platformie, akceptuje warunki korzystania z Platformy, określone w Regulaminie zamieszczonym na stronie internetowej https://platformazakupowa.pl/pn/uksw oraz uznaje go za wiążący.

8. Zamawiający poniżej określa instrukcję korzystania z Platformy Zakupowej w niniejszym postępowaniu:

8.1. w zakładce „Postępowania”, Wykonawca wybiera niniejsze postępowanie korzystając z polecenia „Przejdź” przechodzi odpowiednio do postępowania. Wykonawca może przystąpić do postępowania bez posiadania konta oraz bez logowania, w takim przypadku podczas składania oferty Wykonawca będzie zobowiązany do podania danych umożliwiających jednoznaczną identyfikację użytkownika w postaci: nazwy lub imienia i nazwiska Wykonawcy, nr NIP lub PESEL oraz adresu e-mail. Jednakże zaleca się, aby przed rozpoczęciem wypełniania Formularza składania oferty Wykonawca zalogował się do systemu, a jeżeli nie posiada konta, założył bezpłatne konto. W przeciwnym wypadku Wykonawca będzie miał ograniczone funkcjonalności, np. brak widoku wiadomości prywatnych od Zamawiającego w systemie lub wycofania oferty bez kontaktu z Centrum Wsparcia Klienta.

8.2. jeżeli Wykonawca nie jest zalogowany pojawi się komunikat z wybraniem opcji: kontynuuj jako niezalogowany, zaloguj się lub załóż konto. Jeżeli Wykonawca posiada konto loguje się, natomiast jeżeli Wykonawca nie posiada konta, w celu jego założenia

należy wybrać przycisk „Załóż konto". Następnie uzupełnić wymagane informacje w formularzu rejestracyjnym.

8.3. po wypełnieniu formularza rejestracyjnego pojawi się informacja: Przejdź na swoją skrzynkę e-mailową. Wykonawca powinien otrzymać e-maila o tytule: Potwierdź swoje konto na platformie zakupowej Open Nexus. Wykonawca potwierdza swoją tożsamość, klikając w przycisk Potwierdź konto. Od razu po zweryfikowaniu adresu e-mail przez Wykonawcę, konto jest aktywne i można z niego korzystać.

8.4. składanie oferty i innych dokumentów wymaganych w Ogłoszeniu o zamówieniu oraz SWZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym odbywa się za pośrednictwem Platformy Zakupowej.

8.5. Ofertę należy złożyć do Zamawiającego za pośrednictwem Platformy dostępnej pod adresem: https://platformazakupowa.pl/pn/uksw konkretnie w niniejszym postępowaniu o udzielenie zamówienia za pośrednictwem **formularza do złożenia oferty** widocznego na stronie postępowania.

8.6. W przypadku zastrzeżenia tajemnicy przedsiębiorstwa, dokumenty z **tajemnicą przedsiębiorstwa** powinny zostać złożone na Platformie Zakupowej w formularzu składania oferty w pkt 2 przeznaczonym na zamieszczenie tajemnicy przedsiębiorstwa.

8.7. w przypadku oferty Wykonawca składa dokumenty w formie zaszyfrowanej, dlatego też dokumenty złożone przez Platformę nie są widoczne do momentu odszyfrowania dokumentów przez Zamawiającego, które następuje po upływie terminu składania ofert.

8.8. Wykonawca może także samodzielnie wycofać złożoną ofertę:

8.8.1. Wykonawca posiadający konto na Platformie:
W celu wycofania oferty należy zalogować się i wybrać kafelek „Moje oferty". Następnie należy przejść do historii ofertowania klikając w czarną strzałkę przy wybranej ofercie.
Po przejściu na stronę postępowania, na dole formularza należy przejść do szczegółów oferty, klikając ponownie w czarną strzałkę.
W okienku Historia oferty w postępowaniu należy kliknąć w przycisk „Wycofaj ofertę". System wygeneruje automatyczne potwierdzenie wycofania oferty, które Wykonawca otrzyma na pocztę elektroniczną przypisaną do konta,

8.8.2. Wykonawca nieposiadający konta na Platformie:
Wykonawca nieposiadający konta na Platformie Zakupowej może zmienić swoją ofertę poprzez złożenie kolejnej oferty, podając ten sam adres e-mail. System automatycznie wycofa poprzednią ofertę (o czym Wykonawca zostanie poinformowany drogą e-mailową), następnie Wykonawca otrzyma powiadomienie na elektroniczną skrzynkę pocztową z prośbą o potwierdzenie adresu e-mail. Zweryfikowanie adresu e-mailowego przy ponownie złożonej ofercie będzie zakończeniem procesu złożenia kolejnej oferty.
W przypadku wycofania oferty Wykonawca musi rejestrować się w systemie Platformy Zakupowej i dokonać wycofania oferty zgodnie z instrukcją opisaną powyżej w pkt 7.8.1.

8.9. Wykonawca po upływie terminu składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonych dokumentów.

8.10. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z Platformy, w szczególności za sytuację, gdy zamawiający będzie miał możliwość zapoznania się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego").

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

9. Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z "OBWIESZCZENIEM PREZESA RADY MINISTRÓW z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".

9.1. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na format **.pdf**

9.2. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:

9.2.1. .zip

9.2.2. .7Z

9.3. Wśród formatów powszechnych a NIE występujących w rozporządzeniu występują: **.rar .gif .bmp .numbers .pages.** Dokumenty złożone w takich plikach **zostaną uznane za złożone nieskutecznie.**

10. Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików

składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.

11. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
12. Zamawiający zaleca, aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów może doprowadzić do problemów w weryfikacji plików.
13. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
14. Zaleca się, aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza "Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu email.
15. Zaleca się przygotować ofertę z należytą starannością i z zachowaniem odpowiedniego zapasu czasu do upływu terminu składania ofert.
16. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
17. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
18. Zamawiający zaleca, aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików.
19. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu, w tym zwrotu kosztów poniesionych z tytułu nabycia kwalifikowanego podpisu elektronicznego.
20. Korzystanie z Platformy przez Wykonawcę jest bezpłatne.

XVIII. WYJAŚNIANIE TREŚCI SWZ

1. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ .
2. Wniosek o wyjaśnienie treści SWZ należy przekazać Zamawiającemu za pośrednictwem Platformy Zakupowej.
3. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 14 dni przed upływem terminu składania ofert.
4. Jeżeli Zamawiający nie udzieli wyjaśnień w terminach, o których mowa w ust. 3, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.
5. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ, o którym mowa w ust. 1.
6. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 3, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
7. Treść zapytań wraz z wyjaśnieniami Zamawiający udostępnia, bez ujawniania źródła zapytania, na Platformie Zakupowej.

8. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. W przypadku gdy zmiana treści SWZ jest istotna dla sporządzenia oferty lub wymaga od wykonawców dodatkowego czasu na zapoznanie się ze zmianą treści SWZ i przygotowanie ofert, Zamawiający przedłuża termin składania ofert o czas niezbędny na ich przygotowanie przez zamieszczenie informacji na Platformie Zakupowej.
9. Dokonaną zmianę treści SWZ Zamawiający udostępnia na Platformie Zakupowej.
10. W przypadku gdy zmiana treści SWZ prowadzi do zmiany treści ogłoszenia o zamówieniu, Zamawiający przekazuje Urzędowi Publikacji Unii Europejskiej ogłoszenie, o którym mowa w art. 90 ust. 1 Pzp.

XIX. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą do dnia **04.02.2022,** przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w ust.1, Zamawiający przed upływem terminu związania ofertą, zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 60 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 1, wymaga złożenia przez wykonawcę, za pośrednictwem środków komunikacji elektronicznej wskazanych w Części XVII, pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.
5. Jeżeli termin związania ofertą upłynął przed wyborem najkorzystniejszej oferty, Zamawiający wzywa wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie oraz za pośrednictwem środków komunikacji elektronicznej wskazanych w pisemnej zgody na wybór jego oferty.
6. W przypadku braku zgody, o której mowa w ust. 5, Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.
7. Zamawiający **odrzuca ofertę jeżeli**:
   1) wykonawca nie wyraził pisemnej zgody na przedłużenie terminu związania ofertą;
   2) wykonawca nie wyraził pisemnej zgody na wybór jego oferty po upływie terminu związania ofertą.

XX. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wykonawca może złożyć tylko jedną ofertę w języku polskim.
2. Wykonawcy zobowiązani są zapoznać się dokładnie z informacjami zawartymi w SWZ i przygotować ofertę zgodnie z wymaganiami w niej określonymi.
3. Zaleca się przygotowanie oferty na Formularzu ofertowym, którego wzór stanowi **Załącznik nr 1 do SWZ**. Oferta musi zawierać wszystkie informacje określone w tym Formularzu.
4. Ofertę, oświadczenia, o których mowa w części XVI SWZ ust. 1 -4 o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu (JEDZ-e), wykonawca składa pod rygorem nieważności w formie elektronicznej.
5. W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, Zamawiający żąda od wykonawcy dołączenia do oferty odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru. (Nie dotyczy Wykonawców składających ofertę jako osoby fizyczne).
6. Wykonawca nie jest zobowiązany do złożenia dokumentów, o których mowa w ust. 5, jeżeli Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile wykonawca wskazał w ofercie dane umożliwiające dostęp do tych dokumentów.
7. Jeżeli w imieniu wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów, o których mowa w ust.5, Zamawiający żąda od wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania wykonawcy.
8. Wymaganie określone w ust. 7 stosuje się odpowiednio do osoby działającej w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.
9. Wymagania określone w ust. 5-8 stosuje się odpowiednio do osoby działającej w imieniu podmiotu udostępniającego zasoby lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach.
10. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym wykonawca przekazuje wraz z tłumaczeniem na język polski.
11. Do oferty należy dołączyć dodatkowo:
    1) aktualne na dzień składania ofert odpowiednio oświadczenie/a, o których mowa w części XVI SWZ ust. 1 -4 (JEDZ-e/ESPD, **Załącznik nr 2 do SWZ**)
    2) zobowiązanie podmiotu do udostępnienia zasobów, jeżeli wykonawca polega na zasobach innego podmiotu, (**Załącznik nr 3 do SWZ**)
    3) oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy (jeżeli dotyczy); (**Załącznik nr 4 do SWZ**)
    4) przedmiotowe środki dowodowe, w zakresie, w którym są wymagane;

5) dowody równoważności, o których mowa w części IV SWZ, jeżeli wykonawca zaoferował rozwiązania równoważne w stosunku do określonych w opisie przedmiotu zamówienia;
6) uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa, jeżeli wykonawca zastrzegł w ofercie informacje jako tajemnicę przedsiębiorstwa;
7) opis parametrów technicznych oferowanego sprzętu.

XXI. WADIUM

Zamawiający nie wymaga wniesienia wadium.

XXII. TERMIN SKŁADANIA OFERT, TERMIN OTWARCIA OFERT

1. Termin złożenia oferty **08.11.2021 10:00**
2. Zamawiający zapewnia, aby z zawartością ofert nie można było zapoznać się przed upływem terminu ich otwarcia.
3. Zamawiający dokona otwarcia ofert w dniu **08.11.2021 11:30**, nie później niż następnego dnia po dniu, w którym upłynął termin składania ofert.
4. Otwarcie ofert nie jest jawne i następuje na platformie zakupowej.
5. W przypadku awarii systemu teleinformatycznego przy użyciu, którego Zamawiający otwiera oferty, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
6. Zamawiający informuje o zmianie terminu otwarcia ofert, w stosunku do określonego w ust. 3, na stronie internetowej prowadzonego postępowania.
7. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania, o której mowa w części II SWZ, informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

XXIII. SPOSÓB OBLICZENIA CENY

1. Cena oferty winna obejmować całkowity koszt wykonania zamówienia.
2. Wykonawca jest zobowiązany do wypełnienia formularza pn. „Formularz oferty”, określenia w nim kwot netto i brutto z wyodrębnieniem podatku VAT, z dokładnością do dwóch miejsc po przecinku. Cena oferty winna być wyrażona w pieniądzu – w złotych polskich.
3. Ceny jednostkowe określone przez wykonawcę nie będą podlegały zmianom.
4. Cena oferty stanowi wartość umowy i będzie niezmienna w toku realizacji całej umowy.
5. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2018 r. poz. 2174, z późn. zm.), dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W ofercie, o której mowa w zdaniu pierwszym, wykonawca ma obowiązek:

a. poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;
b. wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
c. wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;
d. wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

XXIV. ODRZUCENIE OFERTY

1. Zamawiający odrzuci ofertę, jeżeli:
1) została złożona po terminie składania ofert;
2) została złożona przez wykonawcę:
   a) podlegającego wykluczeniu z postępowania lub
   b) niespełniającego warunków udziału w postępowaniu, lub
   c) który nie złożył w przewidzianym terminie oświadczenia, o którym mowa w części XVI SWZ ust. 1 -4 (na podstawie art. 125 ust. 1 Pzp), lub podmiotowego środka dowodowego, potwierdzających brak podstaw wykluczenia lub spełnianie warunków udziału w postępowaniu, przedmiotowego środka dowodowego, lub innych dokumentów lub oświadczeń;
3) jest niezgodna z przepisami ustawy;
4) jest nieważna na podstawie odrębnych przepisów;
5) jej treść jest niezgodna z warunkami zamówienia;
6) nie została sporządzona lub przekazana w sposób zgodny z wymaganiami technicznymi oraz organizacyjnymi sporządzania lub przekazywania ofert przy użyciu środków komunikacji elektronicznej określonymi przez zamawiającego;
7) została złożona w warunkach czynu nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
8) zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia;
10) zawiera błędy w obliczeniu ceny lub kosztu;
11) wykonawca w wyznaczonym terminie zakwestionował poprawienie omyłki, o której mowa w art. 223 ust. 2 pkt 3 Pzp;
12) wykonawca nie wyraził pisemnej zgody na przedłużenie terminu związania ofertą;
13) wykonawca nie wyraził pisemnej zgody na wybór jego oferty po upływie terminu związania ofertą;
16) jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;
17) obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe;

XXV. BADANIE OFERT

1. W toku badania i oceny ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert oraz przedmiotowych środków dowodowych lub innych składanych dokumentów lub oświadczeń. Niedopuszczalne jest prowadzenie między Zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty oraz, z uwzględnieniem ust. 2, dokonywanie jakiejkolwiek zmiany w jej treści.
2. Zamawiający poprawia w ofercie:
   1) oczywiste omyłki pisarskie,
   2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   3) inne omyłki polegające na niezgodności oferty z dokumentami zamówienia, niepowodujące istotnych zmian w treści oferty

   – niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.
3. W przypadku, o którym mowa w ust. 2 pkt 3, Zamawiający wyznacza wykonawcy odpowiedni termin na wyrażenie zgody na poprawienie w ofercie omyłki lub zakwestionowanie jej poprawienia. Brak odpowiedzi w wyznaczonym terminie uznaje się za wyrażenie zgody na poprawienie omyłki. W przypadku gdy wykonawca w wyznaczonym terminie zakwestionuje poprawienie omyłki jego oferta zostanie odrzucona na podstawie art. 226 ust.1 pkt 11 Pzp.
4. Jeżeli zaoferowana cena lub koszt, lub ich istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia lub budzą wątpliwości zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów, Zamawiający żąda od wykonawcy wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu, lub ich istotnych części składowych.
5. W przypadku gdy cena całkowita oferty złożonej w terminie jest niższa **o co najmniej 30%** od:
   1) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania lub średniej arytmetycznej cen wszystkich złożonych ofert niepodlegających odrzuceniu na podstawie art. 226 ust. 1 pkt 1 i 10 Pzp, Zamawiający zwraca się o udzielenie wyjaśnień, o których mowa w ust. 4, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia
   2) wartości zamówienia powiększonej o należny podatek od towarów i usług, zaktualizowanej z uwzględnieniem okoliczności, które nastąpiły po wszczęciu postępowania, w szczególności istotnej zmiany cen rynkowych, zamawiający może zwrócić się o udzielenie wyjaśnień, o których mowa w ust. 4.
6. Wyjaśnienia, o których mowa w ust. 4, mogą dotyczyć w szczególności:
   1) zarządzania procesem produkcji, świadczonych usług lub metody budowy;
   2) wybranych rozwiązań technicznych, wyjątkowo korzystnych warunków dostaw, usług albo związanych z realizacją robót budowlanych;
   3) oryginalności dostaw, usług lub robót budowlanych oferowanych przez wykonawcę;

4) zgodności z przepisami dotyczącymi kosztów pracy, których wartość przyjęta do ustalenia ceny nie może być niższa od minimalnego wynagrodzenia za pracę albo minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2018 r. poz. 2177) lub przepisów odrębnych właściwych dla spraw, z którymi związane jest realizowane zamówienie;
5) zgodności z prawem w rozumieniu przepisów o postępowaniu w sprawach dotyczących pomocy publicznej;
6) zgodności z przepisami z zakresu prawa pracy i zabezpieczenia społecznego, obowiązującymi w miejscu, w którym realizowane jest zamówienie;
7) zgodności z przepisami z zakresu ochrony środowiska;
8) wypełniania obowiązków związanych z powierzeniem wykonania części zamówienia podwykonawcy.

7. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na wykonawcy.
8. Odrzuceniu, jako oferta z rażąco niską ceną lub kosztem, podlega oferta wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie, lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej w ofercie ceny lub kosztu.

XXVI. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Za najkorzystniejszą zostanie uznana oferta, która nie zostanie odrzucona na podstawie art. 226 ust. 1 Pzp oraz uzyska maksymalną liczbę punktów na podstawie kryteriów oceny, wymienionych poniżej.
2. Zamawiający przy wyborze oferty będzie kierował się następującymi kryteriami oceny:

Lp.	Nazwa kryterium	Waga % (maksymalna liczba punktów)
1	Cena oferty	55 %
2	Parametry Techniczne	35%

*1) Liczba punktów w kryterium „**Cena oferty**” zostanie wyliczona wg wzoru:*

$$\text{liczba punktów oferty ocenianej} = \frac{\text{cena oferty najniżej skalkulowanej}}{\text{cena oferty ocenianej}} \times \mathbf{55}\ \text{pkt}$$

*2) W kryterium „**Parametry Techniczne**” Liczba punktów zostanie wyliczona w poniższy sposób:*

*a) Podkategoria „**Uczenie maszynowe**”:*
Oferowane rozwiązanie nie posiada tej funkcjonalności – 0 pkt,

*Oferowane rozwiązanie posiada tą funkcjonalność – **15** pkt,*

b) *Podkategoria „**Automatyzacja**”:*
Oferowane rozwiązanie nie posiada tej funkcjonalności – 0 pkt,
*Oferowane rozwiązanie posiada tą funkcjonalność – **10** pkt,*

c) *Podkategoria „**Raportowanie**”:*
Oferowane rozwiązanie nie posiada tej funkcjonalności – 0 pkt,
*Oferowane rozwiązanie posiada tą funkcjonalność – **15** pkt,*

d) *Podkategoria „**Narzędzia do automatyzacji zarządzania infrastrukturą**”:*
Oferowane rozwiązanie nie posiada tej funkcjonalności – 0 pkt,
*Oferowane rozwiązanie posiada tą funkcjonalność – **5** pkt*

Szczegółowy opis spełniania punktowanych funkcjonalności w podkategoriach wyszczególnionych powyżej znajduje się w załączniku numer 5 do SWZ (Opis Przedmiotu zamówienia) w rozdziale IV „Wymagania dodatkowo punktowane”.

Maksymalnie Wykonawca może otrzymać 35 pkt w tym kryterium.

3. Ocenę całkowitą oferty stanowi suma punktów poszczególnych kryteriów – maksymalna ocena to 100 pkt.

XXVII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

Projektowane postanowienia umowy w sprawie zamówienia publicznego dotyczące niniejszego zamówienia stanowią **załącznik nr 6 do SWZ**.

XXVIII. ZAWIADOMIENIE O WYBORZE NAJKORZYSTNIEJSZEJ OFERTY

1. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający informuje równocześnie wykonawców, którzy złożyli oferty, o:
   1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
   2) wykonawcach, których oferty zostały odrzucone
      – podając uzasadnienie faktyczne i prawne.
2. Zamawiający udostępnia niezwłocznie informacje, o których mowa w ust. 1 pkt 1, na Platformie Zakupowej.

3. Zamawiający może nie ujawniać informacji, o których mowa w ust. 1, jeżeli ich ujawnienie byłoby sprzeczne z ważnym interesem publicznym.

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

1. Jeżeli zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający **żąda** przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych wykonawców.
2. Zamawiający **żąda** wniesienia zabezpieczenia należytego wykonania umowy na zasadach określonych w części XXX SWZ.

XXX. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

1. **Zamawiający żąda wniesienia zabezpieczenia należytego wykonania umowy, zwanego dalej „Zabezpieczeniem" w wysokości 3 % ceny oferty**
2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
3. Zabezpieczenie wnosi się przed zawarciem umowy.
4. Zabezpieczenie może być wnoszone, według wyboru wykonawcy, w jednej lub w kilku następujących formach:
   1) pieniądzu;
   2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
   3) gwarancjach bankowych;
   4) gwarancjach ubezpieczeniowych;
   5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
5. Zabezpieczenie wnoszone w pieniądzu wykonawca wpłaca przelewem na rachunek bankowy **Santander Bank Polska S.A. 68 1090 1014 0000 0001 2994 7766 z dopiskiem: „zabezpieczenie należytego wykonania Umowy nr……."**
6. Jeżeli Zabezpieczenie wniesiono w pieniądzu, Zamawiający przechowuje je na oprocentowanym rachunku bankowym. Zamawiający zwraca Zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wykonawcy.
7. W trakcie realizacji umowy wykonawca może dokonać zmiany formy Zabezpieczenia na jedną lub kilka form, o których mowa w ust. 4.
8. Zmiana formy Zabezpieczenia jest dokonywana z zachowaniem ciągłości Zabezpieczenia i bez zmniejszenia jego wysokości.
9. Zamawiający zwraca Zabezpieczenie w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane.

10. Zamawiający pozostawia*/nie pozostawia* na Zabezpieczenie roszczeń z tytułu rękojmi za wady lub gwarancji kwotę 30% Zabezpieczenia.
11. Kwota, o której mowa w ust. **10,** jest zwracana nie później niż w 15. dniu po upływie okresu rękojmi za wady lub gwarancji.

XXXI. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Odwołanie przysługuje na:
1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy;
3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia, mimo że Zamawiający był do tego obowiązany.

2. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej, dalej zwanej „Izbą".
3. 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.
4. 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.
5. Odwołanie wnosi się w terminie 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej[1],
6. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia, wnosi się w terminie 10 dni od dnia zamieszczenia ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub dokumentów zamówienia na stronie internetowej.
7. Odwołanie w przypadkach innych niż określone w ust. 6 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. Jeżeli Zamawiający mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty, odwołanie wnosi się nie później niż w terminie:
    1) 30 dni od dnia zamieszczenia w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia,
    2) 6 miesięcy od dnia zawarcia umowy, jeżeli Zamawiający nie opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia.

[1] 15 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1.

9. Odwołanie zawiera:
   1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);
   2) nazwę i siedzibę Zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;
   3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;
   4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku – numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;
   5) określenie przedmiotu zamówienia;
   6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych;
   7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy;
   8) zwięzłe przedstawienie zarzutów;
   9) żądanie co do sposobu rozstrzygnięcia odwołania;
   10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;
   11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
   12) wykaz załączników.

10. Do odwołania dołącza się:
   1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
   2) dowód przekazania odpowiednio odwołania albo jego kopii Zamawiającemu;
   3) dokument potwierdzający umocowanie do reprezentowania odwołującego.

11. Na orzeczenie Izby oraz postanowienie Prezesa Izby, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
12. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.
13. Skargę wnosi się do Sądu Okręgowego w Warszawie – sądu zamówień publicznych.
14. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 Pzp, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe jest równoznaczne z jej wniesieniem.

XXXII. TERMIN ZAWARCIA UMOWY

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem ust. 3, w terminie nie krótszym niż 10 dni od dnia przesłania zawiadomienia o wyborze

najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej.

2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1 jeżeli złożono tylko jedną ofertę.
3. W przypadku wniesienia odwołania Zamawiający nie może zawrzeć umowy do czasu ogłoszenia przez Izbę wyroku lub postanowienia kończącego postępowanie odwoławcze.
4. Jeżeli wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

XXXIII. UNIEWAŻNIENIE POSTĘPOWANIA

1. Zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli:
   1) nie złożono żadnej oferty albo wszystkie złożone oferty podlegały odrzuceniu;
   2) cena lub koszt najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że zamawiający może zwiększyć tę kwotę do ceny lub kosztu najkorzystniejszej oferty;
   3) w przypadkach, o których mowa w art. 248 ust. 3 Pzp, art. 249 Pzp i art. 250 ust. 2 Pzp, zostały złożone oferty dodatkowe o takiej samej cenie lub koszcie;
   4) wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć;
   5) postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego;
   6) wykonawca nie wniósł wymaganego zabezpieczenia należytego wykonania umowy lub uchylił się od zawarcia umowy w sprawie zamówienia publicznego, z uwzględnieniem art. 263 Pzp.
2. Zamawiający może unieważnić postępowanie o udzielenie zamówienia przed upływem terminu do składania ofert, jeżeli wystąpiły okoliczności powodujące, że dalsze prowadzenie postępowania jest nieuzasadnione.
3. Jeżeli Zamawiający dopuścił możliwość składania ofert częściowych, do unieważnienia w części postępowania o udzielenie zamówienia stosuje się przepisy art. 255–258 Pzp.
4. O unieważnieniu postępowania o udzielenie zamówienia Zamawiający zawiadamia równocześnie wykonawców, którzy złożyli oferty lub zostali zaproszeni do negocjacji – podając uzasadnienie faktyczne i prawne.
5. Zamawiający udostępnia niezwłocznie informacje, o których mowa w ust. 1, na stronie internetowej prowadzonego postępowania.
6. W przypadku unieważnienia postępowania o udzielenie zamówienia z przyczyn leżących po stronie Zamawiającego, wykonawcom, którzy złożyli oferty niepodlegające odrzuceniu, przysługuje roszczenie o zwrot uzasadnionych kosztów uczestnictwa w tym postępowaniu, w szczególności kosztów przygotowania oferty.

7. W przypadku unieważnienia postępowania o udzielenie zamówienia Zamawiający niezwłocznie zawiadamia wykonawców, którzy ubiegali się o udzielenie zamówienia w tym postępowaniu, o wszczęciu kolejnego postępowania, które dotyczy tego samego przedmiotu zamówienia lub obejmuje ten sam przedmiot zamówienia.
8. Zamawiający może unieważnić postępowanie o udzielenie zamówienia, jeżeli środki publiczne, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu przyznane, a możliwość unieważnienia postępowania na tej podstawie została przewidziana w ogłoszeniu o zamówieniu.

XXXIV. ZAŁĄCZNIKI DO SWZ

1. Formularz oferty
2. Oświadczenie wstępne o braku podstaw wykluczenia i spełnianiu warunków udziału w postępowaniu- na formularzu jednolitego dokumentu (JEDZ/ESPD)
3. Zobowiązanie do udostępnienia zasobów
4. Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.
5. Opis Przedmiotu Zamówienia
6. Projektowane postanowienia umowy.
7. Oświadczenie o aktualności braku podstaw wykluczenia
8. Oświadczenie wykonawcy w zakresie przynależności do tej samej grupy kapitałowej (art. 108 ust. 1 pkt 5 Pzp)
9. Wykazy dostaw.

Załącznik nr 1 do SWZ

CNT.371.037.2021

FORMULARZ OFERTY

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

I. Wykonawca:

Niniejsza oferta została złożona przez wykonawcę/wykonawców wspólnie ubiegających się o udzielenie zamówienia:

l.p.	Nazwa(y) Wykonawcy (ów)	Adres(y) Wykonawcy(ów)
1.		
2.		

II. Osoba uprawniona do kontaktów:

Imię i Nazwisko	
Adres	
Telefon	
e-mail:	

III. Warunki oferty:

Odpowiadając na ogłoszenie o zamówieniu w postępowaniu prowadzonym w trybie przetargu nieograniczonego na wykonanie zamówienia pn.

…….

przedkładam niniejszą ofertę i oświadczam/y

1. Oferujemy wykonanie przedmiotu zamówienia za cenę: **cena netto:** ……, [suma pozycji 'wartość netto' RAZY 'ilość sztuk' z punktów 4.1-6 poniżej] (słownie:……) **podatek VAT :** …… (słownie:……) **cena brutto:**……, (słownie:……)
2. Zapoznałem się z specyfikacją warunków zamówienia (SWZ) oraz innymi dokumentami zamówienia oraz zdobyłem wszelkie konieczne informacje do właściwego przygotowania oferty. Przyjmuję przekazane dokumenty bez zastrzeżeń i zobowiązuję się do wykonania przedmiotu zamówienia zgodnie z warunkami w nich zawartymi.
*3. Oferuję niżej wymieniony okres gwarancji i rękojmi:** **Systemy serwerowe TYP 1 – 60 miesięcy** **Systemy serwerowe TYP 2 – 60 miesięcy** **Systemy serwerowe TYP 3 – 60 miesięcy** **Przełączniki Ethernet TYP 1– 60 miesięcy** **Przełączniki Ethernet TYP 2– 60 miesięcy** **Rozwiązanie Firewall – 36 miesięcy**
4. Oferuję: **1) Systemy serwerowe TYP 1 – sztuk 3** **wartość netto za jedną sztukę …….** **2) Systemy serwerowe TYP 2 – sztuk 3** **wartość netto za jedną sztukę …….** **3) Systemy serwerowe TYP 3 – sztuk 3** **wartość netto za jedną sztukę …….** **4) Przełączniki Ethernet TYP 1 – sztuk 2** **wartość netto za jedną sztukę …….** **5) Przełączniki Ethernet TYP 2 – sztuk 4** **wartość netto za jedną sztukę …….** **6) Rozwiązanie Firewall – sztuk 2** **wartość netto za jedną sztukę …….** **Jednoznaczna identyfikacja oferowanego sprzętu znajduje się w tabeli „Jednoznaczna**

identyfikacja wybranych podzespołów".

Informacja o dodatkowo punktowanych elementach znajduje się w tabeli „Jednoznaczna identyfikacja dodatkowo punktowanych elementów"

W załączeniu zamieszczam opis parametrów technicznych oferowanego sprzętu.

5. Oświadczam, że do wykonania przedmiotu zamówienia zastosujemy rozwiązania równoważne w stosunku do opisywanych w opisie przedmiotu zamówienia

TAK/NIE* (zaznacz właściwe)

(w przypadku udzielenia odpowiedzi TAK tj. zastosowania w ofercie rozwiązań równoważnych do oferty należy załączyć dowody równoważności, o których mowa w części IV SWZ;

6. Zobowiązuję się w przypadku wyboru naszej oferty do zawarcia umowy na określonych w SWZ warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

7. Oświadczam, że uważam się za związanego niniejszą ofertą na okres wskazany w SWZ.

8. Oświadczam, że wybór mojej oferty prowadzić będzie do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. 2020 r. poz. 106, z późn. zm.)

TAK/NIE* (zaznacz właściwe),

w przypadku udzielenia odpowiedzi TAK wykonawca podaje:

1) nazwę (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego ……;

2) wartość towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku ……;

3) stawkę podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie ……

9. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO tj. 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa.

10. Oświadczam, iż wykonanie poniższych części zamówienia zamierzam powierzyć następującym podwykonawcom:

1. Nazwa części zamówienia …….
2. Nazwa podwykonawcy, o ile jest znany……

11. Przekazana w odrębnym pliku część oferty stanowi tajemnicę przedsiębiorstwa w rozumieniu art. 11 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. 2020 r. poz. 1913 z późn. zm.). Zastrzegam, że informacje te nie mogą być udostępniane oraz wykazuję, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
(*uzasadnienie należy dołączyć do oferty, jeżeli dotyczy)*

12.Dane umożliwiające dostęp do dokumentów potwierdzających umocowanie do reprezentowania wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia, podmiotów udostępniających zasoby, jeżeli wykonawca z nich korzysta (takie jak np. odpis lub informacja z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub inny właściwy rejestr)
…….
(informacje nieobowiązkowe, dotyczą bezpłatnych i ogólnodostępnych baz danych, na których dostępne są powyższe dokumenty, w przypadku nie podania tych informacji należy dokumenty potwierdzające umocowanie do reprezentowania jw. dołączyć do oferty)

13. Pełnomocnik w przypadku składania oferty wspólnej (jeżeli dotyczy):
Nazwisko, imię .....

14. Wykonawca jest małym □, średnim □, dużym □ przedsiębiorcą (zaznaczyć właściwe)

15. Do niniejszego formularza dołączono następujące dokumenty :

1. **Jednoznaczna identyfikacja wybranych podzespołów**
2. **Jednoznaczna identyfikacja dodatkowo punktowanych elementów**
3. …….
4. …….
5. …….

Jednoznaczna identyfikacja wybranych podzespołów

Nazwa	Jednoznaczna identyfikacja podzespołu (np. numer katalogowy, typ-model, part numer, …)	Nazwa jednoznacznie identyfikująca podzespół odpowiadający wskazanemu identyfikatorowi
Systemy serwerowe TYP 1		
Jednostka CPU		
Pamięć RAM		
Ilość adapterów / portów 25 GbE		
Ilość adapterów / portów 32 Gb		
Ilość i rodzaj dysków		
Systemy serwerowe TYP 2		
Jednostka CPU		
Pamięć RAM		
Ilość adapterów / portów 25 GbE		
Ilość adapterów / portów 32 Gb		
Ilość i rodzaj dysków		
Systemy serwerowe TYP 3		
Jednostka CPU		
Pamięć RAM		
Ilość adapterów / portów 25 GbE		
Ilość i rodzaj dysków		
Przełączniki Ethernet – typ 1		
Ilość portów 1 GbE (RJ45)		
Przełączniki Ethernet – typ 2		
Ilość wkładek 10 GbE		
Ilość wkładek 25 GbE		
Rozwiązanie Firewall		
Ilość interfejsów 40 GbE QSFP+		
Ilość interfejsów 10 GbE SFP+		
Ilość interfejsów 1/10 GbE (RJ45)		

Jednoznaczna identyfikacja dodatkowo punktowanych elementów

Nazwa	**Jednoznaczna identyfikacja podzespołu (np. numer katalogowy, typ-model, part numer, …)**	**Nazwa jednoznacznie identyfikująca podzespół odpowiadający wskazanemu identyfikatorowi**
Uczenie Maszynowe		
Automatyzacja		
Raportowanie		
Dojrzałość rozwiązania		
Automatyzacja zarządzania infrastrukturą		

dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym

Załącznik nr 3 do SWZ

CNT.371.037.2021

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

ZOBOWIĄZANIE DO UDOSTĘPNIENIA ZASOBÓW

Ja: …… (imię i nazwisko osoby upoważnionej do reprezentowania podmiotu udostępniającego zasoby), działając w imieniu i na rzecz:
……
……
(nazwa podmiotu)
Zobowiązuję się do oddania nw. zasobów:
……
……
(określenie zasobu)
do dyspozycji wykonawcy :
……
(nazwa wykonawcy)

na potrzeby realizacji zamówienia pod nazwą:

……

Oświadczam:
1) udostępniam wykonawcy ww. zasoby, w następującym zakresie:
……
2) sposób i okres udostępnienia wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia:
……
3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą:
……

dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym

Załącznik nr 4 do SWZ

CNT.371.037.2021
Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

OŚWIADCZENIE WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA, Z KTÓREGO WYNIKA, KTÓRE ROBOTY BUDOWLANE, DOSTAWY LUB USŁUGI WYKONAJĄ POSZCZEGÓLNI WYKONAWCY (art. 117 ust. 4 Pzp)

Oświadczam w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia, że poszczególni wykonawcy będą wykonywać roboty budowlane, dostawy lub usługi jak w wykazie poniżej:

l.p.	Nazwa wykonawcy wspólnie ubiegającego się o udzielenie zamówienia	Wykonywana przez tego wykonawcę część robót budowlanych, dostaw lub usługi
1.		
2.		
3.		

dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym

Załącznik nr 5 do SWZ

CNT.371.037.2021
Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

OPIS PRZEDMIOTU ZAMÓWIENIA

Miejsce dostawy i instalacji
UKSW,
Centrum Cyfrowej Nauki i Technologii UKSW, ul. Marii Konopnickiej 1, Dziekanów Leśny.

Spis treści

I Systemy serwerowe

Typ 1

Zamawiający wymaga dostarczenia **trzech identycznych serwerów** o parametrach opisanych poniżej:

1. Obudowa typu rack o wysokości max 1U z możliwością instalacji min 10 dysków 2,5" Hot-Plug (w tym minimum 4 NVMe) wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android / Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
2. Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3. Zainstalowane dwa procesory dwunastordzeniowe x86, dedykowane do pracy z zaoferowanym serwerem osiągające w teście SPECspeed2017_fp_base wynik min. 116. Wynik dla oferowanego modelu serwera dostępny na stronie www.spec.org.
4. Wsparcie dla wirtualizacji wspomaganej sprzętowo (KVM), poprzez implementację rozszerzeń bezpośrednio w oferowanym procesorze.
5. 192 GB DDR4 RDIMM 3200 MT/s, na płycie głównej musi być wyposażona w minimum 24 sloty DIMM. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
6. Funkcjonalność pamięci RAM: Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
7. Min. 3 sloty PCIe x16 generacji 4.
8. Interfejsy sieciowe:
    a. Co najmniej dwa interfejsy sieciowe 1GbE w standardzie BaseT
    b. Co najmniej cztery interfejsów sieciowe 25 GbE ze złączami w standardzie SFP28 na co najmniej dwóch fizycznych adapterach (modułach),
    c. Co najmniej cztery porty FC 32 Gb/s, na dwóch fizycznych adapterach (modułach)
    d. Dla opisanych powyżej portów 25 GbE, 32 Gb należy dostarczyć (jeśli konieczne) właściwe wkładki.
9. Możliwość instalacji dysków SATA, SAS, SSD, NVMe.
10. Zainstalowane co najmniej:
    a. 2 dyski o pojemności co najmniej 240 GB SSD o współczynniku DWPD na poziomie co najmniej 3,
    b. 2 dyski o pojemności co najmniej 6.4 TB SSD (NVMe) o współczynniku DWPD na poziomie co najmniej 3,
11. Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64 GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
12. Sprzętowy kontroler dyskowy, posiadający min. 8 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
13. 3xUSB z czego min. 1 port USB 2.0 na przednim panelu obudowy oraz 1 port USB 3.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym),
14. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200
15. Wentylatory redundantne
16. Zasilacze: Redundantne, Hot-Plug min. 1400W każdy.
17. Zintegrowany moduł TPM 2.0.
18. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
19. Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

20. Serwer powinien być zaprojektowany i wyprodukowany w procesie Security Development Lifecycle zgodnym z normą ISO/IEC 27034. Na potwierdzenie tego wymogu wykonawca musi załączyć do oferty oświadczenie producent serwera.
21. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.
22. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
23. Serwer musi posiadać certyfikat bezpieczeństwa EAL-4 o poziomie nie mniejszym niż EAL-4+.
24. Dla zapewnienia odpowiedniego poziomu bezpieczeństwa wszystkie pakiety oprogramowania układowego powinny być podpisane cyfrowo za pomocą hash'a SHA-256 z 2048-bitowym szyfrowaniem. Serwer musi skanować aktualizacje oprogramowania układowego i porównywać ich sygnatury za pomocą wbudowanego w sprzęt łańcucha zaufania.
25. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:
    a. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    b. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
    c. możliwość podmontowania zdalnych wirtualnych napędów
    d. wirtualną konsolę z dostępem do myszy, klawiatury
    e. wsparcie dla IPv6
    f. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH
    g. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer
    h. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
    i. integracja z Active Directory
    j. możliwość obsługi przez dwóch administratorów jednocześnie
    k. Wsparcie dla automatycznej rejestracji DNS
    l. wsparcie dla LLDP
    m. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
    n. możliwość zarządzania bezpośredniego poprzez port USB umieszczony na froncie obudowy.
    o. możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,
26. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
    a. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
    b. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
    c. Wsparcie dla protokołów WMI, SNMP, IPMI, WSMan, Linux SSH,
    d. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
    e. Szczegółowy opis wykrytych systemów oraz ich komponentów
    f. Możliwość eksportu raportu do CSV, HTML, XLS,
    g. Grupowanie urządzeń w oparciu o kryteria użytkownika
    h. Szybki podgląd stanu środowiska
    i. Podsumowanie stanu dla każdego urządzenia
    j. Szczegółowy status urządzenia/elementu/komponentu
    k. Generowanie alertów przy zmianie stanu urządzenia.
    l. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
    m. Integracja z service desk producenta dostarczonej platformy sprzętowej
    n. Możliwość przejęcia zdalnego pulpitu
    o. Możliwość podmontowania wirtualnego napędu
    p. Kreator umożliwiający dostosowanie akcji dla wybranych alertów
    q. Możliwość importu plików MIB
    r. Przesyłanie alertów „as-is" do innych konsol firm trzecich

s. Możliwość instalacji sterowników i aktualizacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
t. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
u. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
v. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych

27. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-50001. Serwer musi posiadać deklaracja CE.
Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012 R2, Microsoft Windows 2016, Microsoft Windows 2019.
28. Serwer musi być w pełni obsługiwany przez system operacyjny Linux/UNIX wspierany przez producenta oferowanych komponentów, bez ograniczeń na liczbę użytkowników. System operacyjny musi w pełnym zakresie wspierać wszystkie komponenty serwerów, w szczególności posiadać niezbędne sterowniki. System operacyjny musi być 64-bitowy.
29. **Pięć lat gwarancji producenta** z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
30. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
31. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
32. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
33. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Typ 2

Zamawiający wymaga dostarczenia **trzech identycznych serwerów** o parametrach opisanych poniżej:

1. Obudowa Rack o wysokości max 2U z możliwością instalacji minimum 16 dysków 2,5" Hot-Plug (w tym minimum 8 NVMe) wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android / Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
2. Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3. Zainstalowane dwa procesory szesnastordzeniowe x86, dedykowane do pracy z zaoferowanym serwerem osiągające w teście SPECrate2017_int_base wynik min. 281. Wynik dla oferowanego modelu serwera dostępny na stronie www.spec.org.
4. Wsparcie dla wirtualizacji wspomaganej sprzętowo (KVM), poprzez implementację rozszerzeń bezpośrednio w oferowanym procesorze.
5. 1 TB DDR4 RDIMM 3200 MT/s, na płycie głównej musi być wyposażona w minimum 32 sloty DIMM. Płyta główna powinna obsługiwać do min. 4 TB pamięci RAM.
6. Funkcjonalność pamięci RAM: Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling

7. Min. 8 uniwersalnych slotów generacji 4, w tym co najmniej 2 sloty o prędkości x16.
8. Interfejsy sieciowe:
    a. Co najmniej dwa interfejsy sieciowe 1GbE w standardzie BaseT
    b. Co najmniej osiem interfejsów sieciowych 25 GbE ze złączami w standardzie SFP28 na co najmniej czterech fizycznych adapterach (modułach),
    c. Co najmniej cztery porty FC 32 Gb/s, na dwóch fizycznych adapterach (modułach)
    d. Dla opisanych powyżej portów 25 GbE, 32 Gb należy dostarczyć (jeśli konieczne) właściwe wkładki.
9. Możliwość instalacji dysków SATA, SAS, SSD, NVMe.
10. Zainstalowane co najmniej:
    a. 2 dyski M.2 SATA o pojemności co najmniej 240 GB oraz możliwość skonfigurowania w RAID 1 (Hot-Plug),
11. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
12. Sprzętowy kontroler dyskowy, posiadający min. 8 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
13. 4xUSB (minimum 2 port USB 2.0 oraz 2 porty USB 3.0), możliwość rozbudowy o Serial Port
14. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
15. Wentylatory redundantne
16. Zasilacze: Redundantne, Hot-Plug min. 1400W każdy.
17. Zintegrowany moduł TPM 2.0.
18. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
19. Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
20. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
21. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
22. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera
23. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
24. Serwer powinien być zaprojektowany i wyprodukowany w procesie Security Development Lifecycle zgodnym z normą ISO/IEC 27034. Na potwierdzenie tego wymogu wykonawca musi załączyć do oferty oświadczenie producent serwera.
25. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.
26. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
27. Serwer musi posiadać certyfikat bezpieczeństwa EAL-4 o poziomie nie mniejszym niż EAL-4+.
28. Serwer musi umożliwiać utworzenia bezpiecznego profilu w oparciu o konfigurację sprzętową i wewnętrznego oprogramowania komponentów serwera. Jakiekolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi.
29. Dla zapewnienia odpowiedniego poziomu bezpieczeństwa wszystkie pakiety oprogramowania układowego powinny być podpisane cyfrowo za pomocą hash'a SHA-256 z 2048-bitowym szyfrowaniem. Serwer musi skanować aktualizacje oprogramowania układowego i porównywać ich sygnatury za pomocą wbudowanego w sprzęt łańcucha zaufania
30. Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
31. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:

a. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
b. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
c. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
d. możliwość podmontowania zdalnych wirtualnych napędów
e. wirtualną konsolę z dostępem do myszy, klawiatury
f. wsparcie dla IPv6
g. wsparcie dla WSMAN (Web Service for Management), SNMP; IPMI2.0, SSH, Redfish
h. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,
i. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
j. integracja z Active Directory
k. możliwość obsługi przez ośmiu administratorów jednocześnie
l. Wsparcie dla dynamic DNS
m. wsparcie dla LLDP
n. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
o. możliwość zarządzania bezpośredniego poprzez port USB umieszczony na przednim panelu serwera,
p. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera,

32. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
    a. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
    b. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
    c. Wsparcie dla protokołów WMI, SNMP, IPMI, WSMan, Linux SSH,
    d. Możliwość oskryptowania procesu wykrywania urządzeń,
    e. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
    f. Szczegółowy opis wykrytych systemów oraz ich komponentów
    g. Możliwość eksportu raportu do CSV, HTML, XLS,
    h. Grupowanie urządzeń w oparciu o kryteria użytkownika
    i. Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń,
    j. Szybki podgląd stanu środowiska
    k. Podsumowanie stanu dla każdego urządzenia
    l. Szczegółowy status urządzenia/elementu/komponentu
    m. Generowanie alertów przy zmianie stanu urządzenia.
    n. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
    o. Integracja z service desk producenta dostarczonej platformy sprzętowej
    p. Możliwość przejęcia zdalnego pulpitu
    q. Możliwość podmontowania wirtualnego napędu
    r. Kreator umożliwiający dostosowanie akcji dla wybranych alertów
    s. Możliwość importu plików MIB
    t. Przesyłanie alertów „as-is” do innych konsol firm trzecich
    u. Aktualizacja oparta o wybrane źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
    v. Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta
    w. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
    x. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych,
33. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-50001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i

posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012 R2, Microsoft Windows 2016, Microsoft Windows 2019.

34. Serwer musi być w pełni obsługiwany przez system operacyjny Linux/UNIX wspierany przez producenta oferowanych komponentów, bez ograniczeń na liczbę użytkowników. System operacyjny musi w pełnym zakresie wspierać wszystkie komponenty serwerów, w szczególności posiadać niezbędne sterowniki. System operacyjny musi być 64-bitowy.
35. Pięć lat gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
36. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego
37. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
38. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
39. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
40. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
41. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Typ 3

Zamawiający wymaga dostarczenia **trzech identycznych serwerów** o parametrach opisanych poniżej:

1. Obudowa Rack o wysokości max 2U z możliwością instalacji minimum 16 dysków 2,5" Hot-Plug (w tym minimum 8 NVMe) wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android / Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
2. Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3. Zainstalowane dwa procesory szesnastordzeniowe x86, dedykowane do pracy z zaoferowanym serwerem osiągające w teście SPECrate2017_int_base wynik min. 281. Wynik dla oferowanego modelu serwera dostępny na stronie www.spec.org.
4. Wsparcie dla wirtualizacji wspomaganej sprzętowo (KVM), poprzez implementację rozszerzeń bezpośrednio w oferowanym procesorze.
5. 384 GB DDR4 RDIMM 3200 MT/s, na płycie głównej musi być wyposażona w minimum 32 sloty DIMM. Płyta główna powinna obsługiwać do min. 4 TB pamięci RAM.
6. Funkcjonalność pamięci RAM: Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
7. Min. 8 uniwersalnych slotów generacji 4, w tym co najmniej 2 sloty o prędkości x16.
8. Interfejsy sieciowe:
    a. Co najmniej dwa interfejsy sieciowe 1GbE w standardzie BaseT
    b. Co najmniej osiem interfejsów sieciowych 25 GbE ze złączami w standardzie SFP28 na co najmniej czterech fizycznych adapterach (modułach),
    c. Dla opisanych powyżej portów 25 GbE należy dostarczyć (jeśli konieczne) właściwe wkładki.
9. Możliwość instalacji dysków SATA, SAS, SSD, NVMe.

10. Zainstalowane co najmniej:
    a. 8 dysków NVME generacji 4, o pojemności co najmniej 6.4 TB o współczynniku DWPD na poziomie co najmniej 3,
    b. 2 dyski M.2 SATA o pojemności co najmniej 240 GB oraz możliwość skonfigurowania w RAID 1 (Hot-Plug),
    c. 16 dysków SAS 2,4 TB HDD 10k.
11. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 16GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
12. Sprzętowy kontroler dyskowy, posiadający min. 8 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
13. 4xUSB (minimum 2 port USB 2.0 oraz 2 porty USB 3.0), możliwość rozbudowy o Serial Port
14. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
15. Wentylatory redundantne
16. Zasilacze: Redundantne, Hot-Plug min. 1400W każdy.
17. Zintegrowany moduł TPM 2.0.
18. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
19. Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
20. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
21. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
22. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera
23. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
24. Serwer powinien być zaprojektowany i wyprodukowany w procesie Security Development Lifecycle zgodnym z normą ISO/IEC 27034. Na potwierdzenie tego wymogu wykonawca musi załączyć do oferty oświadczenie producent serwera.
25. Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.
26. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
27. Serwer musi posiadać certyfikat bezpieczeństwa EAL-4 o poziomie nie mniejszym niż EAL-4+.
28. Serwer musi umożliwiać utworzenia bezpiecznego profilu w oparciu o konfigurację sprzętową i wewnętrznego oprogramowania komponentów serwera. Jakiekolwiek odchylenie od profilu musi zostać automatycznie zgłoszone administratorowi.
29. Dla zapewnienia odpowiedniego poziomu bezpieczeństwa wszystkie pakiety oprogramowania układowego powinny być podpisane cyfrowo za pomocą hash'a SHA-256 z 2048-bitowym szyfrowaniem. Serwer musi skanować aktualizacje oprogramowania układowego i porównywać ich sygnatury za pomocą wbudowanego w sprzęt łańcucha zaufania
30. Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
31. Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet umożliwiająca:
    a. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    b. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
    c. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika
    d. możliwość podmontowania zdalnych wirtualnych napędów
    e. wirtualną konsolę z dostępem do myszy, klawiatury

f. wsparcie dla IPv6
g. wsparcie dla WSMAN (Web Service for Management), SNMP; IPMI2.0, SSH, Redfish
h. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer
i. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
j. integracja z Active Directory
k. możliwość obsługi przez ośmiu administratorów jednocześnie
l. Wsparcie dla dynamic DNS
m. wsparcie dla LLDP
n. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
o. możliwość zarządzania bezpośredniego poprzez port USB umieszczone na przednim panelu serwera,
p. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera,

32. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
    a. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
    b. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
    c. Wsparcie dla protokołów WMI, SNMP, IPMI, WSMAn, Linux SSH,
    d. Możliwość oskryptowania procesu wykrywania urządzeń,
    e. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
    f. Szczegółowy opis wykrytych systemów oraz ich komponentów
    g. Możliwość eksportu raportu do CSV, HTML, XLS,
    h. Grupowanie urządzeń w oparciu o kryteria użytkownika
    i. Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń,
    j. Szybki podgląd stanu środowiska
    k. Podsumowanie stanu dla każdego urządzenia
    l. Szczegółowy status urządzenia/elementu/komponentu
    m. Generowanie alertów przy zmianie stanu urządzenia.
    n. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
    o. Integracja z service desk producenta dostarczonej platformy sprzętowej
    p. Możliwość przejęcia zdalnego pulpitu
    q. Możliwość podmontowania wirtualnego napędu
    r. Kreator umożliwiający dostosowanie akcji dla wybranych alertów
    s. Możliwość importu plików MIB
    t. Przesyłanie alertów „as-is” do innych konsol firm trzecich
    u. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
    v. Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta
    w. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
    x. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych,
33. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-50001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Microsoft Windows 2016, Microsoft Windows 2019.
34. Serwer musi być w pełni obsługiwany przez system operacyjny Linux/UNIX wspierany przez producenta oferowanych komponentów, bez ograniczeń na liczbę użytkowników. System operacyjny musi w pełnym zakresie wspierać wszystkie komponenty serwerów, w szczególności posiadać niezbędne sterowniki. System operacyjny musi być 64-bitowy.

35. Pięć lat gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.
36. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
37. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
38. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
39. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
40. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
41. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

II Przełączniki Ethernet

Typ 1

Zamawiający wymaga dostarczenia **dwóch przełączników** o następujących wymaganiach minimalnych:

1. Minimum 48 portów 10/100/1000 BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) oraz uplink 4x 10 GbE SFP
2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
    a. Gigabit Ethernet 1000Base-T,
    b. Gigabit Ethernet 1000Base-SX,
    c. Gigabit Ethernet 1000Base-LX/LH,
    d. Gigabit Ethernet 1000Base-EX,
    e. Gigabit Ethernet 1000Base-ZX,
    f. Gigabit Ethernet 1000Base-BX-D/U,
    g. 10Gigabit Ethernet 10GBase-SR,
    h. 10Gigabit Ethernet 10GBase-LR,
    i. 10Gigabit Ethernet 10GBase-ER,
    j. 10Gigabit Ethernet 10GBase-ZR,
    k. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
3. Wszystkie porty aktywne, gotowe do obsługi urządzenia końcowego, z pełną obsługą Power over Ethernet (PoE).
4. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    a. Przepustowość w ramach stosu – 80 Gb/s
    b. Do 8 urządzeń w stosie
    c. Zarządzanie poprzez jeden adres IP
    d. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5. Przełącznik musi być wyposażony w moduł do łączenia w stos wraz z kablem stackującym o długości co najmniej 50 cm.
6. Przełączniki muszą być ze sobą połączone tak, aby tworzyć jeden segment sieci. Zamawiający wymaga dostarczenia wszystkich komponentów i licencji jeśli są potrzebne do zrealizowania funkcjonalności.
7. Przepustowość przełącznika (*switching capacity*) co najmniej:

   a. 176 Gb/s (bez podłączenia do stosu)
   b. 256 Gb/s (z podłączeniem do stosu)
8. Prędkość przesyłania (*forwarding rate*) co najmniej: 130.95 Mpps
9. Bufor pakietów: co najmniej 6MB
10. Pamięć DRAM: co najmniej 2 GB
11. Pamięć Flash: co najmniej 4 GB
12. Obsługa minimum:
   a. 500 aktywnych sieci VLAN
   b. 16 000 adresów MAC
   c. 3 000 tras IPv4
   d. 1 500 tras IPv6
   e. 1 000 wpisów w listach kontroli dostępu (Security ACL)
   f. 1 000 wpisów w listach kontroli dostępu QoS ACL
   g. 512 interfejsów SVI L3
   h. 9198 B Jumbo Frame
   i. 48 połączeń zagregowanych typu „port channel”
   j. 16 linków w ramach połączenia zagregowanego typu „port channel” LACP
13. Wsparcie dla:
   a. Obsługi protokołu NTP
   b. Obsługi IGMP v1/2/3 i MLD v1/2 Snooping
   c. Obsługi protokołu LLDP i LLDP-MED.
   d. Funkcjonalności Layer 2 traceroute umożliwiającej śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
   e. Obsługi funkcji Voice VLAN umożliwiającej odsepaowanie ruchu danych i ruchu głosowego
   f. Możliwości uruchomienia funkcji serwera DHCP.
   g. Mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
      i. IEEE 802.1w Rapid Spanning Tree
      ii. Per VLAN Rapid Spanning Tree (PVRST+)
      iii. IEEE 802.1s Multi-Instance Spanning Tree
      iv. Obsługa 64 instancji protokołu STP
   h. Funkcjonalności lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
   i. Funkcjonalności wzorców konfiguracji portów zawierających prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
   j. Funkcjonalności sondy IP SLA Responder.
   k. Próbkowania (bez samplowania) i eksport statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16 000 strumieni (flow).
   l. Realizacji rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstwy 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
   m. Możliwości tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
14. Wymagane mechanizmy związane z bezpieczeństwem sieci:
   a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
c. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
g. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
k. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
l. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
m. Obsługa list kontroli dostępu (ACL) następujących typów:
    i. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    ii. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samej sieci VLAN w obrębie przełącznika,
    iii. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    iv. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),
n. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1 ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACSec Key Agreement (MKA)
o. Wbudowane mechanizmy ochrony własnej kontrolnej przełącznika (CoPP – Control Plane Policing)
p. Funkcja Private VLAN

15. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:
    a. Sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia
    b. Bezpieczna sekwencja uruchamiania
    c. Sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia
16. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

   d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów:
      i. źródłowy/docelowy adres MAC,
      ii. źródłowy/docelowy adres IP,
      iii. źródłowy/docelowy port TCP
   e. Możliwość ograniczenia pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limit)
   f. Kontrola sztormów dla ruchu broadcast /multicast/unicast
   g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
17. Obsługa protokołów i mechanizmów routingu:
   a. Routing statyczny dla IPv4 i IPv6
   b. Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes
   c. Policy-based routing (PBR)
   d. Obsługa protokołu redundantnej bramy (VRRP) z obsługą 64 grup
   e. Obsługa 10 tuneli GRE (Generic Routing Encapsulation)
18. Port konsoli – dedykowany port Ethernet do zarządzania out-of-band
19. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji konfiguracji w pamięci nieulotnej możliwość uruchomienia z nową konfiguracją.
20. Obsługa protokołów SNMPv3, SSHv2, SCP, SFTP (SSH File Transfer Protocol), HTTP, Syslog
21. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów.
22. Wsparcie dla protokołu RESTCONF,
23. Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych
24. Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
25. Port USB umożliwiający podłączenie zewnętrznego nośnika danych oraz możliwość uruchomienia urządzenia z nośnika danych umieszczonego w porcie USB.
26. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki.
27. Możliwość montażu w szafie rack 19''. Wysokość urządzenia nie więcej niż 1 RU. Przełącznik musi być wyposażony w zasilacz podstawowy oraz zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego. Zasilacze wymienne (możliwość instalacji / wymiany „na gorąco" – *hot swap*). Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia. Redundantne wentylatory.
28. Urządzenie wyposażone jest w licencję subskrypcyjną na wymagane funkcjonalności na okres 5 lat.
29. Pięcioletnie wsparcie serwisowe producenta urządzenia w trybie 8/5/NBD. Przez cały okres trwania wsparcia musi być możliwość zgłaszania usterek w systemach serwisowych producenta wraz z możliwością uzyskania pomocy inżynierów producenta.

Typ 2

Zamawiający wymaga dostarczenia **czterech identycznych** urządzeń o następujących minimalnych parametrach:

1. Przełącznik typu standalone wyposażony w 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP.
2. Porty SFP/SFP+/SFP28 umożliwiają zastosowanie następujących wkładek interfejsowych:
   a. Gigabit Ethernet 1000Base-T,
   b. Gigabit Ethernet 1000Base-SX,
   c. Gigabit Ethernet 1000Base-LX/LH,
   d. Gigabit Ethernet 1000Base-EX,

e. Gigabit Ethernet 1000Base-ZX,
f. Gigabit Ethernet 1000Base-BX-D/U,
g. 10Gigabit Ethernet 10GBase-SR,
h. 10Gigabit Ethernet 10GBase-LR,
i. 10Gigabit Ethernet 10GBase-ER,
j. 10Gigabit Ethernet 10GBase-ZR,
k. 10Gigabit Ethernet 10GBase-BX-D/U,
l. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
m. 25Gigabit Ethernet 25GBASE-SR,
n. 25Gigabit Ethernet typu twinax (SFP28 – SFP28),
o. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
p. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);

3. Porty QSFP umożliwiają zastosowanie następujących modułów interfejsowych:
   a. Dla transmisji 40 Gb/s:
      i. 40G-SR4,
      ii. 40G-LR4,
      iii. 40G-ER4,
      iv. 40G-SR-BD,
      v. 40G-CSR,
      vi. 40G-CSR4,
      vii. 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),
      viii. adapter 40G QSFP->10G SFP+,
      ix. 40Gigabit Ethernet typu twinax (QSFP - QSFP);
   b. Dla transmisji 100 Gb/s:
      i. 100GBASE-SR4
      ii. 100GBASE-LR4
      iii. 100 Gigabit Ethernet typu twinax (QSFP-QSFP)
4. Zamawiający wymaga dostarczenia do każdego przełącznika:
   a. 16 modułów 10 GbE SR,
   b. 32 modułów 25 GbE SR.
5. Urządzenie musi posiadać 32MB bufor pamięci, 16GB pamięci DRAM i 16 GB pamięci flash.
6. Przepustowość przełącznika (switching capacity) co najmniej 3,2 Tbps.
7. Prędkość przesyłania (forwarding rate) wynosi co najmniej 1 miliard pps (1Bpps).
8. Urządzenie jest przygotowane do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stackowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie z punktu widzenia protokołów L2 i L3.
9. Przełączniki muszą być ze sobą połączone parami tak, aby tworzyć jeden segment sieci. Zamawiający wymaga dostarczenia wszystkich komponentów i licencji jeśli są potrzebne do zrealizowania funkcjonalności.
10. Obsługa, wsparcie i funkcjonalność dla:
    a. 1 000 aktywnych sieci VLAN
    b. 80 000 adresów MAC
    c. 212 000 tras IPv4
    d. 212 000 tras IPv6
    e. 27 000 wpisów w listach kontroli dostępu Security ACL
    f. 16 000 wpisów w listach kontroli dostępu QoS ACL
    g. 1 000 interfejsów SVI L3
    h. 9198 B Jumbo Frame
    i. 128 połączeń zagregowanych typu „port channel”
    j. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
    k. Protokołu NTP

l. IGMPv1/2/3
m. Standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika
n. wgrywania poprawek bez konieczności restartowania platformy (funkcjonalność systemu operacyjnego przełącznika)
o. konfigurowania systemu operacyjnego przełącznika poprzez API za pomocą m.in. protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
p. wsparcia dla protokołu RESTCONF
q. uruchamiania zdefiniowanych w języku Python skryptów w chwili zaistnienia określonego zdarzenia
r. Realizacja przez przełącznik następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
    i. IEEE 802.1w Rapid Spanning Tree
    ii. Per VLAN Rapid Spanning Tree (PVRST+)
    iii. IEEE 802.1s Multi-Instance Spanning Tree
    iv. Obsługa 1 000 instancji protokołu STP
s. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED.
t. Funkcja serwera DHCP
u. Translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji
v. Realizacji protkołu LISP zgodnie z RFC 6830
w. Enkapsulacji ruchu przy pomocy VXLAN'ów.
x. Funkcjonalności lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
y. Funkcjonalności zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN).
z. Funkcjonalności sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: DHCP, DNS, FTP, http, ICMP-ECHO, ICMP-JITTER, TCP-CONNECT, UDP-ECHO, UDP-JITTER
aa. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
    i. Statycznie w oparciu o port, do którego podłączona jest stacja,
    ii. Statycznie w oparciu o VLAN, w którym pracuje stacja
    iii. Statycznie w oparciu o adres IP stacji,
    iv. Dynamicznie w oparciu o autoryzacje użytkownika / stacji przy pomocy 802.1X
bb. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
cc. Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa

dd. Realizacji sprzętowego tworzenia statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi co najmniej 98 000.
ee. Realizacji rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstwy 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
ff. Możliwości tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.

11. Urządzenie musi realizować następujące funkcjonalności z zakresu MPLS:
    a. L2VPN – Ethernet over MPLS (EoMPLS) – obsługa do 1 000 połączeń wirtualnych VC,
    b. L2VPN – Virtual Private LAN Services (VPLS) – obsługa 1 000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji
    c. L3 VPN – MPLS Virtual Private Network (VPN)
    d. Multicast VPN (MVPN)
12. Obsługa 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
13. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+.
14. Obsługa list kontroli dostępu (ACL) następujących typów:
    a. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    b. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samej sieci VLAN w obrębie przełącznika,
    c. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    d. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),
15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)
16. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:
    a. Sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia
    b. Bezpieczna sekwencja uruchamiania
    c. Sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia
17. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów:
        i. źródłowy/docelowy adres MAC,
        ii. źródłowy/docelowy adres IP,
        iii. źródłowy/docelowy port TCP
    e. Możliwość ograniczenia pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limit)

f. Kontrola sztormów dla ruchu broadcast /multicast/unicast

18. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
19. Urządzenie realizuje routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
    a. Routing statyczny dla IPv4 i IPv6,
    b. Routing dynamiczny dla IPv4: OSPF, BGP, ISIS, EIGRP (rfc7868),
    c. Routing dynamiczny dla IPv6: OSPFv3,
    d. Funkcjonalności Policy-based routing, multicast routing (PIM-SM, PIM-SSM) ,
    e. Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup,
    f. Obsługa 200 tuneli GRE (Generic Routing Encapsulation),
    g. Obsługa 1000 wirtualnych instancji routingu (VRF),
20. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD.
21. Urządzenie posiada dedykowany port Ethernet do zarządzania out-of-band.
22. Port USB umożliwiający podłączenie zewnętrznego nośnika danych oraz możliwość uruchomienia urządzenia z nośnika danych umieszczonego w porcie USB.
23. Obsługa protokołów SNMPv3, SSHv2, SCP, HTTP, Syslog – z wykorzystaniem protokołów IPv4 i IPv6.
24. Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych
25. Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
26. Możliwość montażu w szafie rack 19''. Wysokość urządzenia nie więcej niż 1 RU. Przełącznik musi być wyposażony w zasilacz podstawowy oraz zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego. Zasilacze wymienne (możliwość instalacji / wymiany „na gorąco" – *hot swap*). Urządzenie jest wyposażone w wymienne moduły wentylatorów. Urządzenie może zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1
27. Urządzenie wyposażone jest w licencję subskrypcyjną na wymagane funkcjonalności na okres 5 lat.
28. Pięcioletnie wsparcie serwisowe producenta urządzenia w trybie 8/5/NBD. Przez cały okres trwania wsparcia musi być możliwość zgłaszania usterek w systemach serwisowych producenta wraz z możliwością uzyskania pomocy inżynierów producenta.

III Systemy bezpieczeństwa

Urządzenia wielofunkcyjne

Zamawiający wymaga dostarczenia **dwóch identycznych urządzeń** o parametrach minimalnych wyspecyfikowanych poniżej dla każdego urządzenia:

1. Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". Wszystkie komponenty programowe i sprzętowe muszą posiadać wsparcie od jednego producenta.
2. Urządzenie musi być wyposażone w
   2.1. 4 interfejsy 40GbE QSFP+
   2.2. 4 interfejsy 1/10GbE (RJ45)
   2.3. 16 interfejsów 10GbE SFP+
3. Urządzenie musi być wyposażone w dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w moduł Lights Out Management (LOM) lub odpowiednik

pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania).

4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   4.1. Minimum 16 Gbps dla Firewall/kontroli aplikacji
   4.2. Minimum 8 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware
   4.3. Minimum 150 tys. nowych połączeń na sekundę.
   4.4. Minimum 4 000 000 równoległych sesji
5. Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
6. Jako scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus, antyspyware, ochrony DNS.
7. Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy:
   7.1. rutera (tzn. w warstwie 3 modelu OSI),
   7.2. przełącznika (tzn. w warstwie 2 modelu OSI),
   7.3. w trybie pasywnego nasłuchu (sniffer)
8. Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).
9. Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
10. Urządzenie musi umożliwiać translację adresów IP (NAT) statyczną i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
11. Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych (co najmniej MS Windows, Linux, iOS, Android) musi odbywać się na bazie technologii SSL VPN.
12. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
    12.1. Minimum 10 Gbps dla IPSEC VPN
    12.2. Minimum 5 000 tuneli IPSEC VPN (site-to-site)
    12.3. Minimum 5 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.
13. Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentication) i zastosowanie tego mechanizmu w politykach.
    13.1. Polityki definiujące powinny umożliwiać wykorzystanie
        13.1.1. adresów źródłowych,
        13.1.2. adresów docelowych,
        13.1.3. użytkowników,

13.1.4. numerów portów usług
13.1.5. kategorie URL.
13.2. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia
13.2.1. RADIUS lub TACACS+,
13.2.2. LDAP,
13.2.3. SAML 2.0 lub Kerberos

14. Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej
14.1. oznaczania pakietów znacznikami DiffServ,
14.2. utworzenia co najmniej 8 klas ruchu sieciowego,
14.3. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.
15. Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
16. Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPFv2, OSPFv3 oraz BGP.
17. Urządzenie musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu.
18. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych firewalli/systemów/domen/. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:
18.1. tablic routingu
18.2. polityk bezpieczeństwa obejmujących
18.2.1. System IPS
18.2.2. System ochrony antymalware/antyspyware
18.2.3. System ochrony antywirus
18.3. koncentratorów VPN dla zdalnego dostępu
19. Urządzenie musi wspierać mechanizm PBR (policy based routing) – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
20. Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
21. Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać
21.1. strefy bezpieczeństwa,
21.2. adresy IP klientów i serwerów,
21.3. protokoły i usługi sieciowe,
21.4. aplikacje,
21.5. użytkowników aplikacji,
21.6. kategorie URL
21.7. reakcje zabezpieczeń,
21.8. rejestrowanie zdarzeń
21.9. zarządzanie pasmem QoS.
22. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz obsługę minimum 500 stref bezpieczeństwa.
23. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.

24. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
25. Zamawiający dopuszcza aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania.
26. Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
27. Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja lub per port. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
28. Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
29. Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji
30. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download"
31. Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
32. Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH
33. Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:
    33.1. Microsoft Active Directory,
    33.2. usługi katalogowe LDAP,
    33.3. serwery Terminal Services.
    33.4. informacje z logów SYSLOG
34. Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
35. Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia.

36. Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia.
37. Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na silnik antyspyware w chwili zakupu urządzenia.
38. Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). Baza domen musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 40 milionów rekordów DN. Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia
39. Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie wbudowanej analityki (wykraczającej poza statyczną listę wskazującą CC botnetów).
40. Urządzenie musi posiadać funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia.
41. Urządzenie musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, rar, 7z, bat, ps1, vbs, js) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej

przez złośliwy plik po zainstalowaniu na komputerze końcowym. Zamawiający wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia.

42. Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
43. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:
    43.1. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu
    43.2. Operator, który ma możliwość tylko odczytu konfiguracji.
44. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą
    44.1. bazy lokalnej,
    44.2. serwera LDAP,
    44.3. RADIUS lub TACACS+
    44.4. SAML 2.0
45. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. LDAP -> RADIUS -> baza lokalna)
46. Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Realizacja tego wymagania musi opierać się o samo urządzenie – nie dopuszcza się realizacji koncepcji kandydackiej z wykorzystaniem centralnej konsoli zarządzania. Funkcja ta musi być dostępna również w przypadku utraty komunikacji z centralną konsolą zarządzania. Funkcja ta musi być realizowana co najmniej przez graficzny interfejs zarządzania firewallem (GUI).
47. Urządzenie musi zapewniać interfejs API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Urządzenie musi wspierać co najmniej jeden z poniższych rodzajów API
    47.1. JSON,
    47.2. REST,
    47.3. XML.
48. Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
49. Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
50. Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
51. Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.

Konsola zarządzania dla warstwy firewalli

Poniższe punkty zawierają wymagania minimalne:

1. Wraz z urządzeniami firewall konieczne jest dostarczenie centralnego systemu zarządzania, logowania i raportowania jako systemu realizującego funkcje zbierania logów, zarządzania uprawnieniami administratorów, zarządzania firewallami i inwentury oraz generowania raportów.
2. Zamawiający dopuszcza zaoferowanie systemu zarządzania pochodzącego od jednego producenta składającego się z oddzielnych modułów logowania i zarządzania przy jednoczesnym założeniu, iż każdy element składowy systemu spełni wymagania dotyczące liczby zarządzanych firewalli, przestrzeni dyskowej na logi oraz liczby obsługiwanych logów/zdarzeń na sekundę.
3. Poza wskazaną sytuacją Zamawiający nie dopuszcza oferowania systemu zarządzania składającego się z dwóch lub więcej komponentów niezależnie czy pochodzą od jednego czy wielu producentów.
4. System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej pracującej w środowisku KVM.
5. Zamawiający dopuszcza oferowanie rozwiązań sprzętowych (jako dedykowane appliance oferowane i serwisowane wraz z systemem zarządzania przez producenta), jednakże wówczas w konfiguracji należy przewidzieć docelowe wielkości przestrzeni dyskowej.
6. System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne
   6.1. obsługa nie mniej niż 10 firewalli fizycznych
   6.2. obsługa nie mniej niż 100 firewalli wirtualnych (w rozumieniu wirtualny kontekst/domena/system uruchomiony na dostarczanym firewallu)
   6.3. obsługa co najmniej 8 000 logów/zdarzeń na sekundę (moduł logowania i raportowania)
   6.4. obsługa co najmniej 100 logów/zdarzeń na sekundę – (moduł zarządzania)
   6.5. obsługa przestrzeni dyskowej na logi o pojemności nie mniejszej niż 16 TB jako przestrzeni użytecznej z możliwością rozbudowy o 30%. W przypadku zastosowania dedykowanych urządzeń zarządzania przestrzeń ta musi być dostarczona jako realizowana w RAID-1 lub RAID-6
7. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
8. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
9. System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej:
   9.1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
   9.2. tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego.
   9.3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób
   9.4. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”
10. System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej:
    10.1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu.
       10.1.1. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla)
       10.1.2. globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).

10.2. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów).

10.3. Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń

10.4. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.

10.5. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych

10.6. umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.

11. System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym co najmniej musi

11.1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu

11.2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli.

11.3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur.

11.4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem.

11.5. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów.

11.6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone

11.7. informować o zmianach konfiguracji systemu

12. System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.

Usługa wsparcia technicznego

Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.

Wymagania dotyczące testów weryfikacyjnych oferowanego systemu bezpieczeństwa

Wszelkie czynności związane z postępowanie muszą być dokonane z zachowaniem aktualnych rygorów sanitarnych.

1. Warunkiem podpisania protokołu odbioru sprzętu jest przeprowadzenie przez Wykonawcę poniżej opisanej procedury testowej.
2. Zamawiający wymaga przeprowadzenia testów weryfikacyjnych oferowanych rozwiązań. Celem przeprowadzenia procedury testowej jest weryfikacja zgodności urządzeń i oprogramowania z wymaganiami zamawiającego i określonymi przez Wykonawcę w ofercie parametrami.

3. Wszelkie testy będą przeprowadzane przez Wykonawcę w ramach zaoferowanej ceny i na ryzyko Wykonawcy. Zamawiający nie dopuszcza, aby ich przeprowadzenie w jakikolwiek sposób obciążało Zamawiającego.
4. Wszystkie testy będą odbywać się w obecności przedstawicieli Zamawiającego i przedstawicieli Wykonawcy. Testy muszą być prowadzone w języku polskim lub angielskim.
5. Zamawiający wymaga, aby Wykonawca przygotował opis metodyki prowadzenia testów, zgodnie z warunkami opisanymi poniżej, w szczególności jednoznacznie wyspecyfikował sprzęt i oprogramowanie, których zamierza użyć w testach weryfikacyjnych.
6. Wykonawca zobowiązany jest do przekazania opisu (metodologii) testów (zgodnie z warunkami opisanymi poniżej) Zamawiającemu najpóźniej na trzy dni przed planowanym terminem testów w celu akceptacji zgodności zaproponowanej metodyki testów z wymaganiami OPZ.
7. Czas trwania testów nie może przekroczyć 6 godzin zegarowych. Zamawiający zobowiązuje Wykonawcę do przeprowadzenia testów w siedzibie Zamawiającego. Wykonawca będzie miał prawo do przygotowania środowiska testowego na miejscu testów na dwie godziny zegarowe przed rozpoczęciem testów.
8. Zamawiający wymaga, aby Wykonawca przeprowadził testy na dostarczonych egzemplarzach oferowanego firewalla.
   8.1. Zamawiający wymaga oprogramowania systemowego w wersji zaoferowanej przez Wykonawcą w ofercie (oprogramowanie poziomu General Availability). Zamawiający nie dopuszcza wykorzystania w testach wersji specjalnych oprogramowania.
   8.2. Wymagane są do przeprowadzenia testów wszystkie licencje (Zamawiający dopuszcza licencje testowe, jednakże bez ograniczeń funkcjonalnych na czas prowadzenia testów).
   8.3. Dokumentację dla dostarczanych elementów i systemów w języku polskim lub angielskim (lub wskazanie publicznie dostępnych stron internetowych z lokalizacją dokumentacji)
9. Zamawiający nie dopuszcza wykorzystania w czasie testów innego modelu urządzenia aniżeli ten który został zaoferowany.
10. W przypadku, gdy do przeprowadzenia ww. testów, niezbędne będzie zastosowanie urządzeń generujących odpowiednie obciążenie urządzenia oraz niezbędna będzie odpowiednia infrastruktura sieciowa, Wykonawca zobowiązany jest do zapewnienia niezbędnego wyposażenia.
11. Testy wydajnościowe muszą być przeprowadzone przy włączonym firewallu aplikacyjnym oraz włączonych mechanizmach bezpieczeństwa, jakie posiada oferowane urządzenie (w szczególności z wymaganymi w Opisie Przedmiotu Zamówienia funkcjami ochrony IPS, ochrony antywirusowej, ochrony przed spyware, z blokowaniem przychodzących plików wykonywalnych) oraz w rekomendowanym przez producenta trybie pracy (optymalizowanym pod kątem ochrony). Zamawiający nie dopuszcza, aby testy wydajnościowe były prowadzone z konfiguracją, w której nastąpi wyłączeniem jakiejkolwiek wymaganej przez Zamawiającego funkcji bezpieczeństwa lub z przełączeniem jakiejkolwiek wymaganej przez Zamawiającego funkcji bezpieczeństwa w tryb obniżający poziom bezpieczeństwa (np. poprzez wyłączenie części sygnatur IPS czy sygnatur antywirusowych, sprawdzanie tylko części ruchu w sesji).
12. Zamawiający wymaga, aby w czasie testów potwierdzających deklarowaną przepustowość wykorzystany został mix ruchu obejmujący protokoły HTTP/HTTPS, IMAP, POP3, SMTP, FTP, DNS. W czasie testów potwierdzających deklarowaną liczbę obsługiwanych jednocześnie sesji Zamawiający wymaga, aby został wykorzystany ruch HTTP.
13. Jeżeli Wykonawca deklaruje spełnienie wymagania dodatkowego w postaci dotyczącego lokalnego zbierania i analizowania logów test musi obejmować również lokalne składowanie logów.

14. **Zamawiający uzna, iż urządzenie spełnia jego wymagania pod kątem wydajnościowym, jeżeli urządzenie w testach weryfikacyjnych uzyska co najmniej 90% wydajności wymaganej przez Zamawiajacego tj 7,2 Gbps oraz 100% liczby obsługiwanych sesji.**
15. Zamawiający zastrzega sobie prawo do zweryfikowania w czasie testów dowolnego parametru czy funkcjonalności opisanej w Opisie Przedmiotu Zamówienia, z uwzględnieniem wymagań dodatkowo punktowanych.
16. Podczas testów Wykonawca zobowiązany jest do udzielenia Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane rozwiązanie posiada wymagane przez Zamawiającego funkcjonalności.
17. W przypadku, gdy Zamawiający stwierdzi, że oferowane rozwiązanie nie posiada wymaganych funkcjonalności (parametrów funkcjonalnych), będzie to podstawą do **odmowy podpisania protokołu odbioru Umowy**.
18. W przypadku, gdy testy weryfikacyjne nie potwierdzą, że oferowane urządzenie posiada deklarowane parametry funkcjonalne, lub jego parametry wydajnościowe będą odbiegały od deklarowanych o więcej niż 10%, będzie to podstawą do **odmowy podpisania protokołu odbioru Umowy**.
19. W przypadku wystąpienia podczas testów problemów lub błędów wykonawca ma prawo do podjęcia czynności zmierzających do ich eliminacji, w szczególności może dokonać niezbędnych z jego punktu widzenia modyfikacji prezentowanego środowiska testowego, w ramach czasu przewidzianego na testy, o którym mowa w opisie powyżej.
20. Po przekroczeniu czasu na testy tj. po upływie 6 godzin zegarowych, zadania, które nie zostały wykonane/zakończone zostaną uznane za niewykonane, i jednocześnie będzie to podstawą do **odmowy podpisania protokołu odbioru Umowy**.
21. Wykonawca zobowiązany jest do przekazania Zamawiającemu wyników testów wydajnościowych w postaci elektronicznej (np. jako dokumenty PDF zapisane na generatorze ruchu) bezpośrednio po zakończeniu testów.

IV Wymagania dodatkowo punktowane

Wymagania dodatkowo punktowane przedstawiają dla Zamawiającego dodatkowa wartość techniczną, nie są bezwzględnie wymagane jako funkcjonalności oferowanych produktów jednakże istotne w zakresie integracji i zapewnienia spójności w zakresie posiadanych i planowanych rozwiązań bezpieczeństwa. Zamawiający przyzna dodatkowe punkty, jeśli Wykonawca spełni wszystkie wymagania opisane punktami wraz ze wszystkimi podpunktami w poszczególnych zakresach.

1. **Uczenie maszynowe - 15 pkt**
   1.1. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach anty-wirus oraz funkcji filtrowania URL. Wymagane jest posiadanie funkcji wykrywania za pomocą ML (Machine Learning) dla następujących danych:
   1.1.1. złośliwych plików wykonywalnych (tzw. PE)
   1.1.2. złośliwych skryptów PowerShell
   1.1.3. złośliwych stron / ataków Phishing
   1.1.4. złośliwych skryptów JavaScript

1.2. Urządzenie musi posiadać funkcję wykrywania nadużyć protokołu DNS do infiltracji i eksfiltracji danych oraz wykrywania złośliwych domen generowanych dynamicznie (tzw. domeny DGA)

2. **Automatyzacja - 10 pkt**
   2.1. Urządzenie Firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
3. **Raportowanie - 15 pkt**
   3.1. W przypadku braku komunikacji z centralną konsolą zarządzania urządzenie musi pozwalać na:
      3.1.1. Lokalne zbieranie i analizowanie logów
      3.1.2. korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:
         3.1.2.1. ruchu sieciowym,
         3.1.2.2. aplikacjach,
         3.1.2.3. zagrożeniach
         3.1.2.4. filtrowaniu stron www.
      3.1.3. tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
      3.1.4. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
   3.2. Urządzenie musi być wyposażone w dyski do przechowywania logów i raportów o pojemności nie mniejszej niż 2 x 400GB
4. **Narzędzia do automatyzacji zarządzania infrastrukturą - 5 pkt**
   4.1. Zamawiający stosuje do zarządzania infrastrukturą narzędzia Terraform i Ansible. Zamawiający wymaga przygotowania kompletu skryptów (programów) do przeprowadzenia wdrożenia dostarczonej infrastruktury z użyciem w/w narzędzi.

V Instalacja, konfiguracja i instruktaż

Zamawiający wymaga realizacji wszystkich zadań przez Wykonawcę w siedzibie Zamawiającego: UKSW Kampus Wóycickiego od poniedziałku do piątku – w godz. 8:30-16:30. Wszystkie zadania muszą być wykonywane w obecności przedstawiciela Zamawiającego. Wykonawca zobowiązany jest do udzielania szczegółowych informacji dotyczących realizowanych czynności na każe zapytanie Zamawiającego (w szczególności – na żądanie - w trybie pisemnym).

Na etapie wdrożenia, w przypadku powzięcia jakichkolwiek wątpliwości dotyczących sposobu implementacji lub działania wdrażanego rozwiązania, Zamawiający ma prawo żądać od Wykonawcy uruchomienia/weryfikacji dowolnej funkcjonalności wchodzącej w skład wdrożenia oraz ma prawo żądać sprawdzenia dowolnego parametru/specyfikacji sprzętu/oprogramowania podlegającego wdrożeniu, a Wykonawca zobowiązuje się do udzielenia wyczerpujących wyjaśnień zaistniałych wątpliwości i uruchomienia/weryfikacji funkcjonalności. W przypadku, gdy Zamawiający stwierdzi, że

oferowane rozwiązanie nie posiada wymaganych funkcjonalności (parametrów funkcjonalnych), będzie to podstawą do **odmowy podpisania protokołu odbioru Umowy**.

Ze względu na charakter i zakres wdrożenia, Zamawiający zobowiązuje Wykonawcę do poufności i zachowania w tajemnicy jakichkolwiek danych związanych z przedmiotowym wdrożeniem i nie ujawniania ich jakimkolwiek podmiotom trzecim na etapie wdrożenia i po jego zakończeniu. Zamawiający zobowiązuje Wykonawcę – po podpisaniu umowy - do prowadzenia komunikacji pisemnej związanej z wdrożeniem tylko i wyłącznie z wyznaczonymi pracownikami Centrum Cyfrowej Nauki i Technologii, w sposób zaszyfrowany po uprzedniej wymianie certyfikatów (kluczy publicznych). Komunikacja musi być prowadzona w sposób zaszyfrowany, imienny i bezpośredni pomiędzy wyznaczonymi pracownikami Zamawiającego i Wykonawcy.

1. Zamawiający wymaga montażu i instalacji wszystkich dostarczonych urządzeń w szafach rack Zamawiającego.
2. Zamawiający wymaga dostarczenia do wyspecyfikowanych komponentów niezbędnego okablowania umożliwiającego podłączenie i poprawną eksploatację dostarczonych produktów. Ponadto zamawiający wymaga, aby wszystkie wyspecyfikowane interfejsy sieciowe były okablowane, aktywne i gotowe do użycia.
3. Przełączniki Ethernet muszą zostać uruchomione, zainicjalizowane oraz wymagana jest konfiguracja połączenia z dostarczonymi serwerami, urządzeniami typu firewall oraz infrastrukturą sieciową zamawiającego. „Przełączniki Ethernet – Typ 1" były połączone ze sobą tak aby tworzyły jeden segment sieci (stack) oraz zostały podłączone do portów 1/10/25 GbE w sieci Zamawiającego. „Przełączniki Ethernet – Typ 2" były połączone ze sobą po dwa tak, aby tworzyły jeden segment sieci (stack). „Przełączniki Ethernet – typ 2" Zostały podłączone do portów 1/10/25 GbE w sieci Zamawiającego Wymagana przepustowość między każdym przełącznikiem „Typ 1" oraz „Typ 2" a siecią zamawiającego nie mniej niż 40 Gb Ethernet. Zamawiający wymaga dostarczenia wymaganego okablowania i elementów niezbędnych do zrealizowania połączenia.
4. Zamawiający wymaga zaplanowania i zaimplementowania planu adresacji IP oraz segmentacji sieci (VLANy) – uzgodnienie na etapie wdrożenia z Zamawiającym.
5. Zamawiający wymaga realizacji okablowania wg wskazań Zamawiającego.
6. Instalacja i konfiguracja klastra urządzeń UTM w środowisku CNT wg szczegółów ustalonych z Wykonawcą na etapie wdrożenia.
7. Zamawiający wymaga realizacji wdrożenia według koncepcji IaC (Infrastructure as Code):
    a. Stosowane przez Zamawiającego narzędzia do automatyzacji zarządzania infrastrukturą zawierają się w narzędziach Terraform i Ansible; Zamawiający preferuje zastosowanie przez Wykonawcę oprogramowania Terraform i Ansible.
    b. Wykonawca zobowiązany jest do dostarczenia bezterminowych licencji wymaganych do stosowania użytych narzędzi IaC (jeśli konieczne)
    c. Wykonawca zobowiązany jest do przekazania skryptów (programów) w otwartej formie tekstowej,
    d. Wykonawca zobowiązany jest do przekazania prawa własności względem przekazanego kompletu skryptów Zamawiającemu; Zamawiający ma prawo do dowolnego modyfikowania i używania skryptów po zakończeniu wdrożenia; Wykonawca w przygotowaniu skryptów, powinien stosować dobre praktyki zawarte w dostępnej dokumentacji technicznej i korzystać ze sprawdzonych, przetestowanych fragmentów kodu (jeśli możliwe), dodając swoją wiedzę ekspercką w opisaniu infrastruktury na potrzeby wdrożenia,
    e. Wykonawca zobowiązany jest do przekazania pełnego kompletu skryptów (programów) wdrożeniowych do Zamawiającego najpóźniej na 5 dni roboczych przed planowanym warsztatem przedwdrożeniowym,
    f. Wykonawca zobowiązany jest do przeprowadzenia warsztatu przedwdrożeniowego, na którym omówi (wyjaśni) w sposób wyczerpujący wszystkie skrypty (programy) przygotowane do przeprowadzenia wdrożenia. Wykonawca zobowiązany jest do

przeprowadzenia warsztatu przedwdrożeniowego najpóźniej na 2 dni robocze przed rozpoczęciem wdrożenia; Czas trwania warsztatu musi być adekwatny do omawianych treści jednak nie krótszy niż 12 godzin zegarowych. Warsztat przedwdrożeniowy musi zakończyć się akceptacją skryptów (programów) przez Zamawiającego,

g. Wykonawca jest zobowiązany do uwzględniania uwag
h. Wykonawca zobowiązany jest do udzielenia wyczerpujących wyjaśnień Zamawiającemu dotyczących dostarczonych skryptów (programów) wdrożeniowych, zarówno na etapie warsztatu jak i na etapie prac wdrożeniowych,
i. Wykonawca może rozpocząć prace wdrożeniowe z wykorzystaniem przygotowanych skryptów (programów) po przeprowadzeniu warsztatu i ich zaakceptowaniu przez Zamawiającego.

8. Zamawiający wymaga instalacji i konfiguracji wg wskazań Zamawiającego (szczegóły uzgodnione na etapie wdrożenia) następujących produktów i usług:
    a. Software Defined Storage (SDS) typu Ceph Storage (open source release) na trzech serwerach TYP3 lub równoważny,
    b. Wirtualizator typu oVirt (open source release) na trzech serwerach TYP2
    c. Trzech instancji serwerów DNS zawartych w trzech różnych systemach fizycznych (lub maszynach wirtualnych z mechanizmem transferu stref na serwerach TYP1 (Zamawiający nie dopuszcza instalacji kontenerowych)
    d. Trzech replikowanych pomiędzy sobą serwerów zarządzania tożsamością w trzech systemach fizycznych (lub maszynach wirtualnych) uruchomionych na trzech serwerach TYP 1. Należy przestrzegać zaleceń technicznych zawartych w dostępnej dokumentacji technicznej produktu. Zamawiający wymaga skonfigurowania co najmniej następujących funkcjonalności:
        i. SSO – uwierzytelnianie i autoryzacja dla dostarczonych systemów operacyjnych, urządzeń sieciowych, modułów zarządzających, usług plikowych (NFS, Samba), serwisu HTTP (Apache)
        ii. Obsługi globalnych katalogów domowych (roaming home)
    e. Dwóch zwirtualizowanych systemów udostępniających system plików wystawiony z SDS poprzez protokoły SMB i NFS w konfiguracji HA (Active/Standby) zintegrowanych z usługą zarządzania tożsamością.
    f. Dwóch instancji centralnego systemu logów i ich konfiguracji wg uzgodnień na warsztatach przedwdrożeniowych,
    g. Instancji GitLab i integacji z usługą zarządzania tożsamością.
9. Zamawiający wymaga dostarczenia wymaganych licencji jeśli są konieczne do wdrożenia zdefiniowanych produktów i usług,
10. Na dostarczonych serwerach musi zostać zainstalowany system operacyjny, właściwy dla instalowanych i konfigurowanych poszczególnych produktów i usług. Wykonawca zobowiązany jest do dostarczenia licencji (jeśli konieczne),
11. Zamawiający wymaga uruchomienia i konfiguracji konsoli zarządzania warstwą firewalli w postaci wirtualnej maszyny.
12. Wykonawca zobowiązany jest do przeprowadzenia instruktażu dla 4 pracowników Zamawiającego, z zakresu produktów i usług dostarczonych w ramach wdrożenia:
    a. Nie mniej niż 8 godzin z zakresu rozwiązania Software Defined Storage,
    b. Nie mniej niż 8 godzin z zakresu wirtualizatora,
    c. Nie mniej niż 6 godzin z zakresu przełączników Ethernet,
    d. Nie mniej niż 8 godzin z zakresu usługi zarządzania tożsamością,
    e. Nie mniej niż 16 godzin z zakresu dostarczonych rozwiązań firewall,
    f. Nie mniej niż 8 godzin dla każdego narzędzia zastosowanego w ramach wdrożenia według koncepcji IaC.
    g. 24 zegarowych godzin konsultacji (bezpośrednich, telefonicznych, telekonferencyjnych) z zakresu wdrożonych produktów i usług, w okresie 3 miesięcy od daty podpisania protokołu odbioru. Przez godzinę zegarową należy rozumieć czas

bezpośredniej pracy z Zamawiającym, nie wlicza się do niego czasu potrzebnego Wykonawcy na przygotowanie merytorycznej odpowiedzi.

13. Zamawiający zobowiązuje Wykonawcę do szczegółowego uzgodnienia zakresu instruktaży z Zamawiającym i uzyskania akceptacji zakresu najpóźniej na 7 dni roboczych przed planowanym przeprowadzeniem instruktaży,
14. Zamawiający wyraża zgodę na wykorzystanie wdrażanego środowiska dla celów realizacji instruktażu, pod warunkiem przywrócenia środowiska do stanu stabilnego i gotowego do użycia po zakończeniu instruktaży,
15. Zamawiający zobowiązuje Wykonawcę do realizacji wszystkich prac, w szczególności wdrożeniowych i instruktażu z zachowaniem zasad reżimu sanitarnego wg bieżącego stanu sytuacji epidemiologicznej i obowiązujących rozporządzeń krajowych i UKSW,
16. Podpisanie protokołu odbioru warunkuje:
    a. przeprowadzenie testów wydajnościowych,
    b. uruchomienie konsoli, poprawne nawiązanie połączenia i możliwość zarządzania urządzeniami typu firewall,
    c. uruchomienie i wymagana zdefiniowanych produktów i usług,
    d. przeprowadzenie instruktażu
    e. wykonanie pełnego płynnego ponownego uruchomienia środowiska (wszystkich dostarczonych komponentów, produktów i usług) przez Zamawiającego

Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego dla Ceph Storage:

1. Oprogramowanie równoważne musi być kompatybilne z wymienionym typem oprogramowania
2. Musi charakteryzować się następującymi cechami równoważności:
    2.1. Zapewniać funkcjonalności zgodne z Ceph Storage w wersji produkcyjnej co najmniej „Luminous” 12.2.8 w tym:
        2.1.1. Wystawianie przestrzeni obiektowej (RADOS)
        2.1.2. Wystawianie przestrzeni blokowej (RBD)
        2.1.3. Wystawianie przestrzeni jako system plików (CephFS)
        2.1.4. Wystawianie przestrzeni za pomocą API zgodnego z S3 (Simple Storage Service) i OpenStack Swift
        2.1.5. Wystawianie przestrzeni za pomocą iSCSI
        2.1.6. Wsparcie dla BlueStore
    2.2. Zapewniać poprawki i aktualizacje
    2.3. Umożliwiać instalację na serwerach z 64 bitowymi procesorami rodziny x86
    2.4. Umożliwiać wystawienie nie mniej niż 80 TB surowej przestrzeni z jednego węzła
    2.5. Umożliwiać korzystanie z narzędzi do automatyzacji zarządzania infrastrukturą
    2.6. Posiadać wsparcie dla standardów bezpieczeństwa w tym m.in. FIPS 140-2 lub standard równoważny

Okres gwarancji zgodnie z informacją w treści powyżej:
Systemy serwerowe TYP 1 – 60 miesięcy
Systemy serwerowe TYP 2 – 60 miesięcy
Systemy serwerowe TYP 3 – 60 miesięcy
Przełączniki Ethernet TYP 1– 60 miesięcy
Przełączniki Ethernet TYP 2– 60 miesięcy
Rozwiązanie Firewall – 36 miesięcy
Okres rękojmi jest równy okresowi gwarancji.

Parametry techniczne stanowią zgodnie z zapisami części XXVI SWZ Kryterium oceny ofert.

Zamawiający przed podpisaniem protokołu odbioru będzie wymagał przeprowadzenia testów potwierdzonych podpisaniem „Protokołu przeprowadzenia testów wydajnościowych”.

Zamawiający wymaga podania w ofercie danych sprzętu wyspecyfikowanych w tabeli „Jednoznaczna identyfikacja wybranych podzespołów”

Zamawiający wymaga podania w ofercie informacji umożliwiających jednoznaczne zweryfikowanie funkcjonalności dodatkowo punktowanych. Zaleca się wypełnienie tabeli „Jednoznaczna identyfikacja dodatkowo punktowanych elementów”. Brak tych informacji w ofercie nie podlega uzupełnieniu i skutkuje brakiem przyznania dodatkowych punktów ofercie wykonawcy.

Załącznik nr 6 do SWZ

CNT.371.037.2021
Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

PROJEKTOWANE POSTANOWIENIA UMOWY

UMOWA NR …….

zawarta w dniu ..... roku w Warszawie pomiędzy:

[*lub w przypadku zawarcia umowy w postaci dokumentu elektronicznego*

Umowa zawarta w dniu złożenia oświadczenia woli przez ostatnią ze stron umowy w formie elektronicznej za pomoc kwalifikowanego podpisu elektronicznego pomiędzy:]

Uniwersytetem Kardynała Stefana Wyszyńskiego w Warszawie,
siedziba: ul. Dewajtis 5, 01-815 Warszawa, REGON: 000001956, NIP: 525-00-12-946
reprezentowanym przez:
……,
zwanym dalej Zamawiającym
a
……,
reprezentowanym przez:
……..

zwana dalej Umową.
Umowa zostaje zawarta w wyniku postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego przeprowadzonego na podstawie art. 132 i nast. ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 ze zm.), zwanej dalej Ustawą.

Znak sprawy: …….

§ 1

1. Przedmiotem Umowy jest dostawa ….. **zwanego dalej Sprzętem** oraz instalacja, uruchomienie i integracja Sprzętu, zgodnie z zapisami OPZ. Szczegółowy opis Przedmiotu Umowy stanowi Opis Przedmiotu Zamówienia (OPZ), uzupełniony o inne istotne informacje o przedmiocie zamówienia stanowiący załącznik numer 1 do Umowy oraz Formularz oferty Wykonawcy oraz opis parametrów technicznych oferowanego sprzętu stanowiący załącznik numer 2 do Umowy.
2. Wykonawca zobowiązuje się, w ramach kwoty określonej w § 3 ust. 1 Umowy, do realizacji zamówienia, zgodnie ze złożoną ofertą oraz Opisem Przedmiotu Zamówienia, w szczególności do:
   1) dostarczenia do Zamawiającego w ramach wynagrodzenia i na ryzyko Wykonawcy nowego, wolnego od wad Sprzętu o jakości i parametrach określonych przez Zamawiającego w Załączniku nr 1 do Umowy i Załączniku nr 2 do Umowy;
   2) dostarczenia Sprzętu do miejsca wskazanego przez Zamawiającego w opakowaniach posiadających wyraźne oznaczenie danego urządzenia (nazwa, liczba sztuk), pozwalających na podpisanie **protokołu dostarczenia przedmiotu zamówienia** (załącznik 3 do Umowy) bez otwierania opakowań;

3) dostarczenia wszystkich niezbędnych akcesoriów i innych drobnych elementów wymaganych do poprawnego działania dostarczanego Sprzętu;
4) wydania instrukcji obsługi, dokumentów gwarancji producenta oraz niezbędnych dokumentów licencyjnych na oprogramowanie oraz dokumentacji powykonawczej.
5) instalacji, uruchomienia i integracji Sprzętu w obecności przedstawiciela Zamawiającego;

§ 2

1. Wykonawca zobowiązuje się wykonać przedmiot umowy **w terminie …..**
2. Miejscem wykonania przedmiotu umowy będzie ….. . Szczegółowy termin i miejsce dostarczenia Wykonawca uzgodni z przedstawicielem Zamawiającego, wskazanym w ust. 4 telefonicznie lub e-mailem. Gotowość do wykonania dostawy zostanie zgłoszona e-mailem z wyprzedzeniem co najmniej 2 dni roboczych.
3. Dostawa odbędzie się w dni robocze, w godzinach 8:00–14:00.
4. Dla celów realizacji Umowy Zamawiający ustanawia następujących przedstawicieli:
   1) w zakresie dostawy - ……..……
   2) w zakresie odbioru jakościowego - ……
5. Dla celów realizacji niniejszej umowy Wykonawca ustanawia następujących przedstawicieli:
   1) w zakresie dostawy - ……..……
   2) w zakresie odbioru jakościowego - ……
6. Wykonanie przedmiotu umowy zostanie potwierdzone podpisaniem protokołu odbioru przedmiotu umowy przez Strony Umowy lub przez przedstawiciela Zamawiającego wskazanego w ust. 4.

§ 3

1. **Całkowita wartość zamówienia wynosi zgodnie z ceną całkowitą podaną w ofercie: …… zł netto plus podatek VAT 23 % w kwocie: …….. zł, co stanowi łącznie …… zł brutto (słownie …).**
2. Wynagrodzenie, jest wynagrodzeniem ryczałtowym w rozumieniu art. 632 Kodeksu cywilnego, obejmującym wszystkie czynności niezbędne do prawidłowego wykonania Umowy. Wykonawca nie może żądać podwyższenia wynagrodzenia.
3. Faktura zostanie wystawiona po podpisaniu **protokołu odbioru przedmiotu umowy** przez Strony Umowy lub przez Zamawiającego (załącznik numer 3 do Umowy).
4. Zamawiający zrealizuje płatność przelewem na rachunek bankowy Wykonawcy, wskazany na fakturze, w terminie do 30 dni od daty dostarczenia prawidłowo wystawionej faktury VAT do siedziby Zamawiającego.
5. Zamawiający zgodnie z ustawą z dnia 9 sierpnia 2019 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw faktury, których wartość brutto będzie przekraczać 15.000,00zł (lub jej równowartość) dokumentujących transakcje, których przedmiotem będą towary i usługi wymienione w załączniku nr 15 do ustawy o VAT - obejmie obowiązkowym mechanizmem podzielonej płatności (split payment).
6. Wykonawca oświadcza, że rachunek bankowy wskazany na fakturze jest rachunkiem umożliwiającym płatność w ramach mechanizmu podzielonej płatności, jak również jest rachunkiem znajdującym się w elektronicznym wykazie podmiotów prowadzonym od 1 września 2019 r. przez Szefa Krajowej Administracji Skarbowej, o którym mowa w ustawie o podatku od towarów i usług (dalej: Wykaz).
7. W przypadku gdy rachunek Wykonawcy nie spełnia warunków określonych w ust. 6 powyżej, opóźnienie w dokonaniu płatności w terminie określonym w ust. 4 powyżej, powstałe w skutek

braku możliwości realizacji przez Zamawiającego płatności wynagrodzenia z zastosowaniem mechanizmu podzielonej płatności bądź dokonania płatności na rachunek objęty Wykazem, nie stanowi dla Wykonawcy podstawy do żądania od Zamawiającego jakichkolwiek odsetek, jak również innych rekompensat / odszkodowań / roszczeń z tytułu dokonania nieterminowej płatności.

8. Za termin dokonania płatności strony przyjmują datę obciążenia rachunku bankowego Zamawiającego.
9. Wszelkie rozliczenia pomiędzy Zamawiającym a Wykonawcą będą dokonywane **w złotych polskich.**

§ 4

1. W przypadku przekroczenia terminu wykonania przedmiotu umowy, określonego w § 2 ust. 1 Umowy przez Wykonawcę, Zamawiający naliczy karę umowną w wysokości 0,1% kwoty brutto określonej w § 3 ust. 1 Umowy za każdy dzień zwłoki.
2. Kara, o której mowa w ust. 1, nie jest naliczana, jeśli zwłoka wynika z winy Zamawiającego, za okres, w którym za zwłokę odpowiada Zamawiający
3. Jeżeli zwłoka w dostarczeniu sprzętu, nie licząc okresu zwłoki, za którą odpowiada Zamawiający, przekroczy 7 dni, Zamawiający może odstąpić od umowy, a Wykonawca zobowiązany jest do zapłaty kary umownej w wysokości 10% kwoty brutto określonej w § 3 ust. 1 Umowy.
4. W przypadku odstąpienia od umowy przez Zamawiającego z powodu niewykonania lub nienależytego wykonania umowy przez Wykonawcę, Wykonawca jest zobowiązany do zapłaty kary umownej na wypadek odstąpienia w wysokości 10% kwoty brutto określonej w § 3 ust. 1 Umowy.
5. W przypadku, o którym mowa w ust. 4, umowne prawo odstąpienia od umowy, przysługuje Zamawiającemu po upływie dodatkowo wyznaczonego terminu 14 dni licząc od terminu określonego w § 2 ust. 1 Umowy.
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 powzięcia wiadomości o tych okolicznościach.
7. W przypadku, o którym mowa w ust. 6 Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
8. Kary umowne Zamawiający ma prawo potrącić bezpośrednio z faktury VAT wystawionej przez Wykonawcę lub z kwoty zabezpieczenia należytego wykonania umowy. Zamawiający poinformuje Wykonawcę na piśmie, o fakcie pomniejszenia wynagrodzenia Wykonawcy, w związku z powstaniem obowiązku zapłaty kar umownych lub potrąceniem kar z zabezpieczenia.
9. W przypadku, gdy wysokość należnych kar umownych nie pokrywa wysokości szkody powstałej na skutek niewykonania lub nienależytego wykonania umowy, niezależnie od zastrzeżonych kar umownych, Zamawiający może dochodzić odszkodowania uzupełniającego na zasadach ogólnych kodeksu cywilnego.
10. Wykonawca zobowiązuje się do zapłaty kar umownych w terminie 14 dni od dnia doręczenia wezwania.
11. W przypadku naliczenia kar umownych z przyczyn, o których mowa w § 6 ust. 4 Umowy, Wykonawca będzie zobowiązany do zapłaty kary umownej na podstawie noty obciążeniowej wystawionej przez Zamawiającego.

12. Odpowiedzialność odszkodowawczą Stron wynikającą z Umowy wyłączają jedynie zdarzenia siły wyższej, których nie można było przewidzieć i którym, jak również ich skutkom, nie można było zapobiec.
13. Przez siłę wyższą, o której mowa w ust. 12, należy rozumieć przypadki lub zdarzenia zewnętrzne, które są poza kontrolą i niezawinione przez żadną ze Stron, których nie można przewidzieć, ani uniknąć, a które zaistnieją po wejściu Umowy w życie i staną się przeszkodą w realizacji zobowiązań umownych.
14. Strona powołująca się na stan siły wyższej jest zobowiązana do powiadomienia drugiej Strony, a następnie do udokumentowania zaistnienia tego stanu.
15. Wystąpienie siły wyższej, poinformowanie o tym Strony oraz udokumentowanie powoduje zawieszenie wykonania zobowiązań umownych o czas trwania siły wyższej.
16. W rozumieniu postanowień ust. 14 i 15 umowy siłą wyższą nie są w szczególności deficyt sprzętowy, kadrowy, materiałowy, spory pracownicze, strajki, trudności finansowe ani też kumulacja takich czynników.
17. Wykonawca, jak i Zamawiający będą czynić starania w kierunku zmniejszenia strat i szkód, jakie mogą powstać w wyniku zaistnienia siły wyższej.
18. Kary za zwłokę w usunięciu wad stwierdzonych w okresie rękojmi lub gwarancji w wysokości 0,05 %. kwoty brutto określonej w § 3 ust. 1Umowy za każdy rozpoczęty dzień zwłoki.
19. Limit Kar z tytułu odstąpienia od umowy wynosi 10% kwoty brutto określonej w § 3 ust. 1 Umowy.
20. Łączna wysokość naliczonych Wykonawcy przez Zamawiającego na podstawie Umowy kar umownych nie przekroczy 20% kwoty brutto określonej w § 3 ust. 1 Umowy
21. Łączna odpowiedzialność odszkodowawcza Wykonawcy, w tym z tytułu kar umownych, na podstawie Umowy nie przekroczy 100% kwoty brutto określonej w § 3 ust. 1 Umowy.
22. W przypadku nieterminowej zapłaty wynagrodzenia, Wykonawca może naliczyć Zamawiającemu odsetki ustawowe na zasadach ogólnych, z zastrzeżeniem postanowień § 3 ust. 7 Umowy.

§ 5

1. Wykonawca udziela Zamawiającemu **gwarancji na okres ……..**
2. Termin rękojmi za wady jest równy okresowi gwarancji zgodnie z art. 558 Kodeksu cywilnego.
3. Termin gwarancji i rękojmi za wady rozpoczyna swój bieg od dnia podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy.
4. Gwarancja oraz rękojmia obejmuje zapewnienie, że urządzenia posiadają parametry techniczne zgodne
z określonymi w Załączniku nr 1 do Umowy oraz w Załączniku nr 2 do Umowy. Gwarancja oraz rękojmia obejmuje także w pełni sprawne i bezawaryjne funkcjonowanie tych urządzeń.
5. Wszelkie uszkodzenia, awarie i niesprawne działanie urządzeń Zamawiający będzie zgłaszać Wykonawcy pisemnie lub e-mailem na adres: ……..*(lub. Należy podać inną alternatywną metodę, np.: przez oficjalny portal producenta)*.
6. Za wykonanie naprawy, wymianę urządzeń lub ich części na nowe oraz usunięcie nieprawidłowości w działaniu całkowitą odpowiedzialność ponosi Wykonawca.
7. W przypadku nieusunięcia wad przez Wykonawcę w wymaganych terminach Zamawiający może usunąć stwierdzone wady na koszt Wykonawcy, zachowując jednocześnie wszelkie uprawnienia do naliczenia kar umownych i odszkodowań uzupełniających, jak również uprawnienia wynikające z gwarancji i rękojmi za wady.

8. Niezależnie od uprawnień z gwarancji udzielonej przez Wykonawcę, Zamawiający może korzystać z uprawnień z gwarancji Producenta.
9. Wykonawca zobowiązany jest uzyskać od Producenta oświadczenie gwarancyjne w rozumieniu art. 577 i art. 577^1 Kodeksu cywilnego, zawierające wskazanie Zamawiającego jako beneficjenta uprawnień
z tytułu gwarancji Producenta. Obowiązek ten zostaje wyłączony w przypadku, gdy Wykonawca jest jednocześnie Producentem urządzeń.

§ 6

1. Czynności serwisowe urządzenia w okresie gwarancji będą świadczone przez Wykonawcę nieodpłatnie, o ile uszkodzenia nie nastąpiły z powodu nieprawidłowego użytkowania urządzenia przez Zamawiającego. Czynności serwisowe mogą być wykonywane w siedzibie Zamawiającego w godzinach 08:00 – 15:00 od poniedziałku do piątku z wyłączeniem świąt i dni wolnych od pracy dla Zamawiającego określonych Zarządzeniem Rektora UKSW.
2. Zamawiający może zgłaszać reklamacje do Wykonawcy w sposób określony w § 5 ust. 5 Umowy podając numer seryjny urządzenia oraz powód zgłoszenia.
3. Wykonawca zapewni naprawę urządzenia w terminie **określonym w standardowych warunkach gwarancji producenta, jednak nie dłuższym niż 21 dni** od daty zgłoszenia naprawy gwarancyjnej, niesprawnego działania, uszkodzenia lub awarii urządzenia. W przypadku konieczności sprowadzenia części zamiennych z zagranicy termin ten może zostać przedłużony jednak nie dłużej niż o 20 dni. Uzasadnienie konieczności przedłużenia terminu jest po stronie Wykonawcy.
4. W przypadku niedotrzymania terminu naprawy lub wymiany urządzeń w ramach gwarancji, Zamawiający może naliczyć kary umowne w wysokości 0,1% kwoty brutto zgłoszonego do naprawy lub wymiany urządzenia, za każdy dzień zwłoki.
5. W przypadku wymiany części lub urządzenia na nowe, gwarancja dla danej części lub urządzenia rozpoczyna swój bieg na nowo, licząc od daty podpisania protokołu wymiany gwarancyjnej.

§ 7

1. Wykonawca wniósł zabezpieczenie należytego wykonania umowy w wysokości … % ceny całkowitej podanej w ofercie, tj. kwotę: ……. zł w formie ..... .
2. Zamawiający zwróci Wykonawcy zabezpieczenie należytego wykonania umowy w następujących wysokościach i terminach:
   a) część zabezpieczenia w wysokości ….% zabezpieczenia, stanowiącą gwarancję zgodnego z umową i należytego wykonania Przedmiotu umowy pomniejszoną o ewentualnie naliczone kary umowne – w ciągu 30 dni od podpisania protokołu odbioru Przedmiotu umowy,
   b) pozostałą część zabezpieczenia, w wysokości ….% zabezpieczenia, pomniejszoną w szczególności o ewentualnie naliczone kary umowne – w ciągu 15 dni po upływie okresu rękojmi za wady, rozpoczętego w dniu podpisania protokołu odbioru Przedmiotu umowy.

§ 8

1. Zamawiający przewiduje następujące możliwości dokonania zmian postanowień Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, w szczególności w sytuacjach:

1) zmiany w przepisach prawa lub wykładni jego przepisów;

2) wystąpienia okoliczności (zdarzeń), na które Strony Umowy nie miały wpływu, a okoliczności (zdarzenia) te dotyczyły działania lub zaniechania:

   a) osób trzecich,

   b) organów administracji publicznej,

w stosunku do okoliczności towarzyszących zawarciu Umowy, a wpływających obiektywnie, bezpośrednio lub pośrednio w sposób dalece utrudniający lub czyniący niemożliwym spełnienie świadczeń Stron Umowy, w sposób określony pierwotnie w Umowie;

3) zmiany wartości Umowy – w przypadku zwiększenia bądź zmniejszenia stawek podatku od towarów i usług, dotyczących przedmiotu zamówienia, w wyniku zmiany ustawy z dnia 11 marca 2004 roku o podatku od towarów i usług (Tekst jednolity obwieszczenie z dnia 19 marca 2021: Dz.U. 2021 poz. 685 ze zm.), które wejdą w życie po dniu zawarcia Umowy, a przed wykonaniem przez Wykonawcę obowiązku, po wykonaniu którego Wykonawca jest uprawniony do uzyskania wynagrodzenia. Wynagrodzenie Wykonawcy może ulec odpowiedniemu zwiększeniu bądź zmniejszeniu, jeżeli w wyniku zastosowania zmienionych stawek podatku od towarów i usług ulega zmianie kwota należnego podatku oraz wynagrodzenie Wykonawcy uwzględniające podatek od towarów i usług. Zmiana wartości Umowy w zakresie dotyczącym wynagrodzenia Wykonawcy będzie dokonana w ten sposób, że należne Wykonawcy wynagrodzenie za wykonanie Umowy będzie obliczone z uwzględnieniem stawki VAT obowiązującej w dniu wystawienia faktury VAT;

4) zmiany przedmiotu umowy – w przypadku, gdy produkt stanowiący przedmiot oferty został wycofany z rynku lub zaprzestano jego produkcji, a proponowany przez Wykonawcę produkt posiada nie gorsze cechy, parametry i funkcjonalność:

a) niż produkt będący przedmiotem umowy oraz

b) niż określone dla zmienianego produktu w Specyfikacji istotnych warunków zamówienia;

5) istnieje możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż istniejące w chwili podpisania Umowy.

2. Zamawiający dopuszcza zmianę umowy w zakresie zmiany terminu realizacji zamówienia z przyczyn niezawinionych przez Wykonawcę.

3. W przypadkach określonych w ust. 1 pkt. 4-5 i ust 2 wynagrodzenie Wykonawcy nie ulega zmianie.

4. Wprowadzenie do Umowy zmian, o których mowa w ust. 1 pkt. 4-5 jest warunkowane złożeniem przez Stronę inicjującą zmianę wniosku zawierającego opis propozycji zmiany wraz z uzasadnieniem zmiany.

5. Wprowadzenie do Umowy zmian, o których mowa w ust. 1, wymaga zgody obydwu Stron wyrażonej w drodze pisemnego aneksu do Umowy.

§ 9.

1. Wykonawca zobowiązuje się:

   a) zachować w ścisłej tajemnicy wszelkie informacje techniczne, technologiczne, prawne i organizacyjne, dotyczące drugiej Strony lub uzyskane od drugiej Strony – niezależnie od formy przekazania tych informacji i ich źródła;

   b) wykorzystywać informacje jedynie w celach realizacji Umowy;

   c) podjąć wszelkie niezbędne kroki dla zapewnienia, że żadna z osób otrzymujących informacje nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części stronom trzecim bez uzyskania uprzedniego wyraźnego upoważnienia na piśmie od Zamawiającego, której informacja lub źródło informacji dotyczy;

d) nie kopiować, nie powielać ani w jakikolwiek sposób nie rozpowszechniać jakichkolwiek części otrzymanych informacji od Zamawiającego;

e) traktować jako poufne informacje, co do których zachodzi podejrzenie, że mogą być informacjami poufnymi, aż do momentu określenia ich statusu;

f) traktować informacje poufne zgodnie z ich specyfiką i chronić je przynajmniej w ten sam sposób i w tym samym stopniu w jakim Strony chronią swoje własne informacje tego typu, przy czym informacje obejmujące dane osobowe lub stanowiące tajemnicę przedsiębiorstwa, Wykonawca zobowiązany jest chronić w sposób przewidziany dla ochrony tych informacji przez Zamawiającego, w stopniu w jakim Zamawiający ochrania te informacje.

2. Obowiązki wynikające z ust. 1 znajdują zastosowanie wobec właścicieli, pracowników, podwykonawców, konsultantów, reprezentantów Wykonawcy oraz innych osób mających dostęp do informacji przekazanych przez Zamawiającego w związku z realizacją Umowy.

3. Z chwilą realizacji Umowy (wykonania przedmiotu umowy) lub ustania celu dla jakiego została ona zawarta, Wykonawca zobowiązuje się do całkowitego usunięcia wszystkich informacji poufnych otrzymanych na mocy zobowiązania do zachowania poufności. Wykonawca zobowiązuje się zachować nadal obowiązki wynikające z zobowiązania w zakresie nie ujawniania informacji udostępnionych jemu przez drugą stronę bez względu na upływ czasu. Dane prawnie chronione, w szczególności takie jak dane osobowe oraz informacje stanowiące tajemnicę przedsiębiorstwa zachowują walor poufności bez względu na upływ czasu.

§ 10

1. Wykonawca oświadcza, że:

1) wszelkie utwory w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawach autorskich i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231 ze zm.), jakimi będzie się posługiwał w toku realizacji umowy, a także powstałe w jej trakcie lub wyniku, będą oryginalne, bez niedozwolonych zapożyczeń z utworów osób trzecich oraz nie będą naruszać praw przysługujących osobom trzecim, a w szczególności praw autorskich oraz dóbr osobistych tych osób,

2) do dnia przeniesienia autorskich praw majątkowych będzie wykonywał te prawa wyłącznie dla celów realizacji umowy.

2. Z dniem wytworzenia utworu w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawach autorskich i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231 ze zm.), w ramach wynagrodzenia, o którym mowa w § 3 ust. 1 niniejszej umowy, Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe i prawa pokrewne do nieograniczonego w czasie korzystania z utworów powstałych w ramach niniejszej umowy i rozporządzania nimi, przez czas nieoznaczony na terytorium Polski i poza jej granicami, na wszystkich znanych obecnie i w przyszłości polach eksploatacji.

§ 11

Strony wzajemnie oświadczają, że posiadają zgodę osób, o których mowa w Umowie do przetwarzania ich danych osobowych, tj. imienia, nazwiska, stanowiska służbowego, numeru telefonu oraz adresu e-mail oraz że dane te przetwarzane będą przez każdą z nich wyłącznie dla potrzeb wykonywania Umowy, przez okres jej trwania z uwzględnieniem ustawowych terminów przechowywania dokumentacji dla celów podatkowych – w trybie i na zasadach określonych Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu

takich danych oraz uchylenia dyrektywy 95/46/WE opublikowane w Dzienniku Urzędowym z 2016 r. nr 119, str. 1.

§ 12

1. Wszelkie spory wynikłe w trakcie realizacji Umowy strony zobowiązują się załatwić polubownie, a w przypadku braku takiej możliwości poddają rozstrzygnięciu sądu właściwego dla siedziby Zamawiającego.
2. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
3. Zastosowanie mają przepisy prawa polskiego.
4. W sprawach nieuregulowanych Umową mają zastosowanie, ustawy Prawo zamówień publicznych oraz Kodeks Cywilny.
5. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, z których jeden otrzymuje Wykonawca, a dwa Zamawiający.
6. Integralną część umowy stanowią załączniki:

Załącznik nr 1 – Opis przedmiotu zamówienia,
Załącznik nr 2 – Formularz ofertowy Wykonawcy oraz opis parametrów technicznych oferowanego sprzętu.
Załącznik nr 3 – Protokół Wykonania umowy (wzór),

ZAMAWIAJĄCY: **WYKONAWCA:**

Załącznik nr 1 do umowy nr: ……..

Opis przedmiotu zamówienia

Załącznik nr 2 do umowy nr: ……..

Formularz ofertowy Wykonawcy
oraz
opis parametrów technicznych oferowanego sprzętu.

Załącznik nr 3 do umowy nr: ……..

PROTOKOŁY
WZÓR

Protokół dostarczenia przedmiotu umowy

Sporządzony w …… w dniu ……., pomiędzy:

……. /Wykonawca/
a
……. /Zamawiający/

1. Zamawiający potwierdza dostarczenie przez Wykonawcę przedmiotu zamówienia. Specyfikację, wraz z numerami seryjnymi / katalogowymi podano w tabeli poniżej:

Lp.	Nazwa	Numer seryjny / katalogowy	Ilość

2. Zamawiający sprawdził kompletność dostarczonego przedmiotu zamówienia.
3. **Niniejszy protokół nie jest podstawą do wystawienia przez Wykonawcę faktury.**
4. Niniejszy protokół sporządzono w 2 jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Za Wykonawcę Za Zamawiającego

Protokół przeprowadzenia testów wydajnościowych

Sporządzony w …… w dniu ……, pomiędzy:

……. /Wykonawca/
a
……. /Zamawiający/

Lp.	Parametr	Wartość wymagana (zgodnie z opisem przedmiotu zamówienia)	Wartość uzyskana w testach	Jednostka
1	Wydajność urządzenia	7,2		Gbps
2	Równoległe sesje	4 000 000		Ilość równoległych sesji

Za Wykonawcę

Za Zamawiającego

WZÓR

Protokół odbioru przedmiotu umowy

Sporządzony w …… w dniu ……, pomiędzy:

…….. /Wykonawca/
a
…….. /Zamawiający/

1. Zamawiający potwierdza dostarczenie i uruchomienie przez Wykonawcę przedmiotu zamówienia zgodnie z postanowieniami umowy.
2. Zamawiający sprawdził kompletność dostarczonego przedmiotu zamówienia.
3. **Niniejszy protokół jest podstawą do wystawienia przez Wykonawcę faktury.**
4. Niniejszy protokół sporządzono w 2 jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Za Wykonawcę Za Zamawiającego

Załącznik nr 7 do SWZ

CNT.371.037.2021

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

Dokument składany na wezwanie Zamawiającego

OŚWIADCZENIE O AKTUALNOŚCI BRAKU PODSTAW WYKLUCZENIA

Podmiot składający oświadczenie:

UWAGA: Oświadczenie składa wykonawca, podmiot udostępniający zasoby, jeden z wykonawców wspólnie ubiegających się o zamówienie, w takim samym zakresie jak wykonawca

……..
……
reprezentowany przez:
……
(imię, nazwisko)

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.:

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że informacje zawarte w Jednolitym europejskim dokumencie zamówienia (JEDZ/ESPD), o którym mowa w Części XVI SWZ aktualne na dzień składania ofert w zakresie poniższych podstaw wykluczenia z postępowania, o których mowa w:

1. art. 108 ust. 1 pkt 3 Pzp,
2. art. 108 ust. 1 pkt 4 Pzp, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
3. art. 108 ust. 1 pkt 5 Pzp, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
4. art. 108 ust.1 pkt 6 Pzp,

są nadal aktualne / są nieaktualne*.

(*Niepotrzebne skreślić.)

Uwaga:
W przypadku braku aktualności podanych uprzednio informacji dodatkowo należy złożyć stosowną informację w tym zakresie, w szczególności określić jakich danych dotyczy zmiana i wskazać jej zakres.

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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

dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym

Załącznik nr 8 do SWZ

CNT.371.037.2021

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

Dokument składany na wezwanie Zamawiającego

OŚWIADCZENIE WYKONAWCY W ZAKRESIE PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ (ART. 108 UST. 1 PKT 5 Pzp)

Podmiot składający oświadczenie:

Uwaga:
Oświadczenie dotyczy wykonawcy, a w przypadku wspólnego ubiegania się o zamówienie każdego z tych wykonawców.

……..
……
reprezentowany przez:
……
(imię, nazwisko)
Na potrzeby postępowania o udzielenie zamówienia publicznego pn.:

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie"

Oświadczam, że:

- nie należę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę lub ofertę częściową: **TAK/NIE***

(*zaznacz właściwe)

- należę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę lub ofertę częściową: **TAK/NIE***

(*zaznacz właściwe)

W przypadku złożenia oświadczenia o przynależności wykonawca dołącza dokumenty lub informacje potwierdzające przygotowanie oferty, oferty częściowej niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej.

dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym

Załącznik nr 9 do SWZ

CNT.371.037.2021

WYKAZ DOSTAW

Składany na wezwanie Zamawiającego

WYKAZ WYKONANYCH LUB WYKONYWANYCH USŁUG

dotyczy: postępowania pn.

Dostawa i instalacja infrastruktury komputerowej dla Centralnego Systemu Zarządzania, Monitorowania i Bezpieczeństwa Systemów Teleinformatycznych i Komputerowych w ramach projektu „Multidyscyplinarne Centrum Badawcze Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie”

na potwierdzenie spełniania warunku określonego w pkt. XIII. 1. 4) SWZ przedstawiamy:

Nazwa sprzętu będącego przedmiotem dostawy	Wartość Dostawy	Data wykonania (rozpoczęcie – zakończenie)	Podmiot, na rzecz którego usługa została wykonana

Należy załączyć dowody potwierdzające, że usługi zostały wykonane lub są wykonywane należycie

dokument należy podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym