SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
w postępowaniu o udzielenie zamówienia publicznego
prowadzonym w trybie przetargu nieograniczonego

na

NA DOSTAWĘ URZĄDZEŃ SIECIOWYCH
DLA SĄDU NAJWYŻSZEGO

nr sprawy: KPP IV-0413-42/20

Integralną część niniejszej SIWZ stanowią:

- Opis przedmiotu zamówienia
- Formularz ofertowy
- Wzór umowy
- Wzór oświadczenia w trybie art. 25a ustawy PZP
- Załącznik nr 1
- Załącznik nr 2
- Załącznik nr 3
- Załącznik nr 4

Zamawiający oczekuje, że Wykonawcy zapoznają się dokładnie z treścią niniejszej SIWZ. Wykonawca ponosi ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów oraz przedłożenia oferty nieodpowiadającej wymaganiom określonym przez Zamawiającego.

Warszawa, czerwiec 2020 r.

Spis treści

Rozdział I. Nazwa oraz adres Zamawiającego.

Sąd Najwyższy
pl. Krasińskich 2/4/6, 00-951 Warszawa
tel. (22) 358 84 09, fax (22) 530 90 30
Godziny pracy: 8^{00}-16^{00} od poniedziałku do piątku.

Adres strony internetowej: www.sn.pl

Rozdział II. Tryb udzielenia zamówienia.

1. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 i nast. *ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych*, zwanej dalej „ustawą PZP".
2. W zakresie nieuregulowanym niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ", zastosowanie mają przepisy ustawy PZP.
3. Wartość zamówienia **nie przekracza** równowartości kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 ustawy PZP.

Rozdział III. Opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest dostawa urządzeń sieciowych:
   - 5 szt. przełączników typ I,
   - 2 szt. przełączników typ II,
   - 1 szt. kontrolera sieci bezprzewodowej,
   - 9 szt. punktów dostępowych sieci bezprzewodowej,

   wraz z systemem zarządzania i monitoringu oraz wyposażeniem dodatkowym, mająca na celu modyfikację infrastruktury sieciowej do zmieniających się standardów w siedzibie Sądu Najwyższego.

   W zmodyfikowanej infrastrukturze Zamawiający zamierza wykorzystywać posiadane już przez niego komponenty, stąd wymaganie, żeby oferowane urządzenia były kompatybilne z tymi komponentami, w szczególności z systemem Cisco Identity Services Engine 2.4 (ISE), przełącznikami Cisco Catalyst 3650, Cisco Catalyst 3750X, Cisco Catalyst 2960X, Cisco Catalyst 2960CX, Cisco Catalyst 3560CX, Cisco Catalyst 9300 z licencją DNA Essentials i DNA Premier, punktami dostępowymi Cisco Aironet 2800 oraz modułami światłowodowymi Cisco 10G LRM oraz Cisco 10G SR. Zatem rozwiązaniem równoważnym będzie zastąpienie komponentów infrastruktury sieciowej Zamawiającego niekompatybilnych z oferowanymi przez Wykonawcę produktami, przez dostarczenie i wdrożenie odpowiedników tych komponentów, kompatybilnych z zaoferowanymi rozwiązaniami. Wdrożenie rozwiązania równoważnego musi odbyć się w sposób nieutrudniający pracy sędziom i pracownikom Sądu Najwyższego, tj. od piątku od godziny 16:30 do niedzieli do godziny 23:30 (łącznie 55 godzin).
2. Szczegółowy opis przedmiotu zamówienia znajduje się **Załączniku nr 1** do SIWZ.
3. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych we wzorze umowy stanowiącym **Załącznik nr 3** do SIWZ.
4. Wspólny Słownik Zamówień CPV: 324200000-3.
5. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
6. Zamawiający nie dopuszcza możliwości składania ofert wariantowych w rozumieniu art. 2 pkt 7 ustawy PZP.
7. Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 6 i 7 ustawy PZP.
8. Zamawiający nie przewiduje aukcji elektronicznej.
9. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
10. Zamawiający dopuszcza możliwość powierzenia podwykonawcy lub podwykonawcom wykonania części przedmiotu zamówienia. W takim wypadku:

1) Wykonawca ma obowiązek, zgodnie z art. 36b ust. 1 ustawy PZP, wskazania w ofercie części zamówienia, które zamierza powierzyć podwykonawcom i podania firm (nazw) podwykonawców - brak tej informacji w ofercie oznaczać będzie, że Wykonawca nie będzie korzystał z podwykonawstwa przy realizacji zamówienia;
2) powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia;
3) Zamawiający żąda, by Wykonawca przed przystąpieniem do wykonania zamówienia podał, o ile są już znane, nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi zaangażowanych w wykonywanie części zamówienia, które im zostały powierzone przez Wykonawcę;
4) jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22a ust. 1 ustawy PZP, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

11. Wykonawca zawiadamia Zamawiającego o wszelkich zmianach danych w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację usług.

Rozdział IV. Termin wykonania zamówienia.

Zamawiający wymaga realizacji zamówienia w terminie do 60 dni, licząc od daty podpisania umowy.

Rozdział V. Warunki udziału w postępowaniu.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
   1) nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12-23 oraz ust. 5 pkt 1, 4 i 8 ustawy PZP;
   2) spełniają warunki udziału w postępowaniu dotyczące:
      a) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów:

         Zamawiający nie wyznacza szczegółowego warunku w tym zakresie,
      b) sytuacji ekonomicznej lub finansowej:

         Zamawiający nie wyznacza szczegółowego warunku w tym zakresie,
      c) zdolności technicznej lub zawodowej:

         Zamawiający nie wyznacza szczegółowego warunku w tym zakresie.
2. Wykonawcy występujący wspólnie:
   1) zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego;
   2) składają wspólną ofertę.
3. Podstawy wykluczenia z postępowania. Zamawiający wykluczy z postępowania Wykonawcę:
   1) który nie wykaże, że nie zachodzą wobec niego przesłanki wykluczenia określone w art. 24 ust. 1 pkt 13-23 ustawy PZP;
   2) wobec którego zachodzą przesłanki określone w art. 24 ust. 5 pkt 1, 4 i 8 ustawy PZP, tj.:
      a) w stosunku, do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. - Prawo restrukturyzacyjne (Dz.U. 2019.243 j.t. z późn. zm.) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację

majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. - Prawo upadłościowe (Dz.U. 2017.2344 j.t. z późn. zm.),

b) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1-4 ustawy PZP, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania,

c) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w art. 24 ust. 1 pkt 15 ustawy PZP, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

4. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16-20 lub art. 24 ust. 5 pkt 1, 4 i 8 ustawy PZP, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Zamawiający nie wykluczy wykonawcy z postepowania i ile uzna, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, za wystarczające przedstawione dowody jakich mowa powyżej. Zdania pierwszego nie stosuje się, jeżeli wobec Wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.
5. W przypadkach, o których mowa w art. 24 ust. 1 pkt 19 ustawy PZP, przed wykluczeniem Wykonawcy Zamawiający zapewni mu poprzez stosowne wezwanie, możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji. Zamawiający wskazuje w protokole sposób zapewnienia konkurencji.
6. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

Rozdział VI. Wykaz oświadczeń lub dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

1. Wykonawca na potwierdzenie wykazania braku podstaw do wykluczenia, o których mowa Rozdziale V, składa wraz z ofertą oświadczenie w trybie art. 25a ustawy PZP, wg wzoru określonego w **Załączniku nr 4** do SIWZ.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia oświadczenie o którym mowa wyżej każdy z Wykonawców składa oddzielnie.
3. Jeżeli Wykonawca, powołuje się na zasoby innych podmiotów w celu wykazania spełniania w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w ust. 1.
4. Wykonawca, załączy do oferty poświadczone za zgodność aktualne na dzień złożenia następujące oświadczenia lub dokumenty:
   1) informację z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy PZP, wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
   2) odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw do wykluczenia na postawie art. 24 ust. 5 pkt 1 ustawy PZP;
   3) zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub inny dokument potwierdzający, że Wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;

4) zaświadczenie właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo inny dokument potwierdzający, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub inny dokument potwierdzający, że Wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

5. Inne dokumenty składane przez Wykonawcę:
   1) W terminie **3 dni** od zamieszczenia na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 5 ustawy PZP, Wykonawca przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP. Wraz ze złożeniem oświadczenia Wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej składa każdy z wykonawców.
   2) Dokumenty lub oświadczenia, o których mowa w *rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz.U. 2016.1126 z późn. zm.)*, składane są w oryginale lub kopii dokumentu poświadczonej za zgodność z oryginałem.
6. Wykonawcy zagraniczni:
   1) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej zamiast dokumentów wymienionych w:
      a) ust. 5 pkt 1 - składa informację z odpowiedniego rejestru 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 lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy PZP - dokumenty powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,
      b) ust. 5 pkt 2 - składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert - wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
   2) Jeżeli w kraju miejsca zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 1 lit. a) zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym z względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby - wystawione z odpowiednią datą wymaganą dla tych dokumentów.
   3) Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w pkt 1 lit. a) składa informację z odpowiedniego rejestru, 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 lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym art. 24 ust. 1 pkt 14 i 21 ustawy PZP. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby.
7. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski.
8. Zamawiający żąda od Wykonawcy przedstawienia dokumentów wymienionych w ust. 5 i 6 dotyczących podwykonawcy, któremu zamierza powierzyć części zamówienia, a który nie jest podmiotem, na którego zdolnościach lub sytuacji Wykonawca polega na zasadach określonych w art. 22a ustawy PZP.
9. W przypadku wskazania przez Wykonawcę oświadczeń lub dokumentów, o których mowa w ust. 5 i 6, które znajdują się w posiadaniu Zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych

przez Zamawiającego zgodnie z art. 97 ust. 1 ustawy PZP, Zamawiający w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy PZP, korzysta z posiadanych oświadczeń lub dokumentów, o ile są one aktualne.

10. W przypadku wskazania przez Wykonawcę dostępności oświadczeń lub dokumentów, o których mowa w ust. 5 i 6 w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobierze samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty. W przypadku, gdy pobrane przez Zamawiającego dokumenty nie są w języku polskim Wykonawca zobowiązany jest złożyć tłumaczenie na język polski.
11. Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.

Rozdział VII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Postępowanie prowadzone jest w języku polskim.
2. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje Zamawiający oraz Wykonawcy mogą przekazywać pisemnie lub drogą elektroniczną, za wyjątkiem oferty, umowy oraz oświadczeń i dokumentów wymienionych w Rozdziale VI niniejszej SIWZ (również w przypadku ich złożenia w wyniku wezwania, o którym mowa w art. 26 ust. 3 ustawy PZP) dla których dopuszczalna jest forma pisemna.
3. W korespondencji kierowanej do Zamawiającego Wykonawca winien posługiwać się numerem sprawy określonym w SIWZ.
4. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę pisemnie winny być składane na adres: Sąd Najwyższy Biuro Informatyki, pl. Krasińskich 2/4/6, 00-951 Warszawa.
5. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę drogą elektroniczną winny być kierowane na adres: sni@sn.pl, a faksem na nr (22) 530 90 30.
6. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje przekazane w formie elektronicznej wymagają na żądanie każdej ze stron, niezwłocznego potwierdzenia faktu ich otrzymania.
7. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ.
8. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert (tj. 3 lipca 2020 roku), Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert.
9. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Zamawiający zamieści wyjaśnienia na stronie internetowej, na której udostępniono SIWZ.
10. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w ust. 8.
11. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
12. Zamawiający nie przewiduje zwołania zebrania Wykonawców.
13. Do porozumiewania się z Wykonawcami, zarówno w kwestiach formalnych, jak i merytorycznych, osobą uprawnioną przez Zamawiającego jest Pan Maciej Pajączkowski – Dyrektor Biura Informatyki w Sądzie Najwyższym.

Jednocześnie Zamawiający informuje, że przepisy ustawy PZP nie pozwalają na jakikolwiek inny kontakt - zarówno z Zamawiającym, jak i osobami uprawnionymi do porozumiewania się z Wykonawcami - niż wskazany w niniejszym rozdziale SIWZ. Oznacza to, że Zamawiający nie będzie reagował na inne formy kontaktowania się z nim, w szczególności na kontakt telefoniczny lub/i osobisty w swojej siedzibie.

Rozdział VIII. Wymagania dotyczące wadium.

1. Wykonawca zobowiązany jest wnieść wadium w wysokości 15.500,00 PLN (słownie złotych: piętnaście tysięcy pięćset).
2. Wadium może być wniesione w:
   1) pieniądzu na konto bankowe wskazane w ust. 4;
   2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem 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 (Dz.U. 2019.310 t.j. z późn. zm.)*.
3. Wadium należy wnieść przed upływem terminu składania ofert.
4. Wadium w formie pieniądza należy wnieść przelewem na konto 10 1130 1017 0020 0800 5120 0003, z dopiskiem w tytule przelewu **„Wadium w postępowaniu KPP IV-0413-42/20 na dostawę urządzeń sieciowych dla Sądu Najwyższego”**.
5. Skuteczne wniesienie wadium w pieniądzu następuje z chwilą uznania środków pieniężnych na rachunku bankowym Zamawiającego, o którym mowa ust. 4 przed upływem terminu składania ofert.
6. Z treści gwarancji lub poręczenia winno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego w terminie związania ofertą, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a i 5 ustawy PZP. Tak wnoszone wadium powinno zabezpieczać złożoną ofertę na cały okres związania ofertą, poczynając od dnia składania ofert.
7. Zamawiający wymaga, aby w przypadku wniesienia wadium w formie:
   1) pieniężnej – dokument potwierdzający dokonanie przelewu wadium został załączony do oferty;
   2) innej niż pieniądz - oryginał dokumentu został złożony w oddzielnej kopercie, a jego kopia w ofercie.
8. W przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia w:
   1) pieniądzu - Zamawiający wymaga, aby wpłaty kwoty pieniężnej dokonał jeden spośród Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
   2) formie gwarancji bankowej lub gwarancji ubezpieczeniowej - Zamawiający wymaga aby wszyscy wykonawcy wspólnie ubiegający się o udzielnie zamówienia byli zobowiązani jej postanowieniami;
   3) formie poręczeń bankowych, poręczeń spółdzielczej kasy oszczędnościowo-kredytowej lub poręczeń 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* - Zamawiający wymaga, aby wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia byli zobowiązani jej postanowieniami.
9. Oferta Wykonawcy, który nie wniesie wadium lub wniesie w sposób nieprawidłowy, zostanie odrzucona zgodnie z art. 89 ust.1 pkt 7b ustawy PZP.
10. Okoliczności i zasady zwrotu wadium, jego przepadku oraz zasady jego zaliczenia na poczet zabezpieczenia należytego wykonania umowy określa ustawa PZP.

Rozdział IX. Termin związania ofertą.

1. Wykonawca będzie związany ofertą przez okres **30 dni**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert (art. 85 ust. 5 ustawy PZP).
2. Wykonawca może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy, samodzielnie lub na wniosek Zamawiającego z tym, że Zamawiający może tylko raz, co najmniej na **3 dni** przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż **60 dni**.
3. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.
4. Przedłużenie terminu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwie, z wniesieniem nowego wadium na przedłużony okres związania ofertą. Jeżeli przedłużenie terminu związania ofertą dokonywane jest po wyborze oferty

najkorzystniejszej, obowiązek wniesienia nowego wadium lub jego przedłużenia dotyczy jedynie Wykonawcy, którego oferta została wybrana jako najkorzystniejsza.

Rozdział X. Opis sposobu przygotowywania ofert.

1. Oferta musi zawierać następujące dokumenty i oświadczenia:
   1) wypełniony **Formularz ofertowy**, sporządzony z wykorzystaniem wzoru stanowiącego **Załącznik nr 2** do SIWZ, w języku polskim;
   2) oświadczenie wymienione w Rozdziale VI ust. 1 – **Załącznik nr 4** do SIWZ;
   3) dokument potwierdzający wniesienie wadium;
   4) pełnomocnictwo lub inny dokument, z którego wynika prawo do podpisania oferty oraz podpisania innych dokumentów składanych wraz z ofertą, chyba że Zamawiający może je uzyskać w szczególności 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 (Dz.U. 2017.570 j.t. z późn. zm.)*, a Wykonawca wskazał to wraz ze złożeniem oferty;
   5) pełnomocnictwa do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia, ewentualnie umowa o współdziałaniu, z której będzie wynikać przedmiotowe pełnomocnictwo - pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy, stosownie do art. 23 ust. 2 ustawy PZP - jeżeli zachodzi taka okoliczność.
2. Dokumenty i oświadczenia, o których mowa w ust. 1, powinny być sporządzone z zachowaniem formy pisemnej pod rygorem nieważności, na maszynie do pisania, wydrukowane lub sporządzone inną trwałą i czytelną techniką.
3. Treść oferty musi odpowiadać treści SIWZ.
4. Zaleca się, aby każda zapisana strona oferty była ponumerowana kolejnymi numerami oraz aby oferta zawierała spis treści.
5. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
6. Wykonawca ma prawo złożyć tylko jedną ofertę, zawierającą jedną, jednoznacznie opisaną propozycję. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
7. Zamawiający informuje, iż zgodnie z art. 8 w związku z art. 96 ust. 3 ustawy PZP oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu *ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 2018.419 j.t. z późn. zm.)*, jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępniane i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
8. Zamawiający zaleca, aby informacje zastrzeżone jako tajemnica przedsiębiorstwa były przez Wykonawcę przesłane w oddzielnej kopercie, z oznakowaniem „tajemnica przedsiębiorstwa", oddzielnie od pozostałych, jawnych elementów oferty. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
9. Zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji będzie traktowane, jako bezskuteczne i skutkować będzie zgodnie z uchwałą Sądu Najwyższego z 20 października 2005 r. (sygn. III CZP 74/05) ich odtajnieniem.
10. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji, kiedy Wykonawca oprócz samego zastrzeżenia jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.
11. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone wg takich samych zasad, jak składana oferta, tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA". Koperty oznaczone

„ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian zostaną dołączone do oferty.

12. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia, według tych samych zasad jak wprowadzanie zmian i poprawek.
13. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty, w tym załączników.
14. Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy PZP zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy PZP). Wszelkie niejasności i wątpliwości dotyczące treści zapisów w SIWZ należy zatem wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym w Rozdziale VII niniejszej SIWZ. Przepisy ustawy PZP nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.

Rozdział XI. Miejsce i termin składania i otwarcia ofert.

1. Złożenie oferty w postępowaniu:
   1) Ofertę należy złożyć w siedzibie Zamawiającego przy pl. Krasińskich 2/4/6 w Warszawie – pok. 0N28 Zespół Biura Podawczego do dnia 7 lipca 2020 r., do godziny 9:00 i zaadresować zgodnie z podanym niżej opisem:

Sąd Najwyższy
pl. Krasińskich 2/4/6, 00-951 Warszawa
„Oferta w postępowaniu na dostawę urządzeń sieciowych dla Sądu Najwyższego"
nr sprawy: KPP IV-0413-42/20
Otworzyć na jawnym otwarciu ofert w dniu 7 lipca 2020 r. o godz. 10:00"

   2) Decydujące znaczenie dla oceny zachowania terminu składania ofert ma data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania.
   3) Oferta złożona po terminie wskazanym w pkt 1 nie zostanie otwarta.
2. Otwarcie ofert:
   1) Otwarcie ofert nastąpi w dniu 7 lipca 2020 r., o godzinie 10:00 w siedzibie Zamawiającego, w pokoju 2N37 (pomieszczenie może zostać zmienione na inne, większe, w zależności od liczby chętnych do udziału w otwarciu ofert).
   2) Otwarcie ofert jest jawne. Wykonawcy mogą uczestniczyć w otwarciu ofert. Podczas otwarcia ofert odczytane zostaną informacje, o których mowa w art. 86 ust. 4 ustawy PZP.
   3) Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie internetowej ofert pod adresem:
      http://www.sn.pl/informacjepraktyczne/SitePages/Zamowienia_publiczne.aspx
      informacje dotyczące:
      a) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia,
      b) firm oraz adresów wykonawców, którzy złożyli oferty w terminie,
      c) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach, jeżeli były wymagane.

Rozdział XII. Opis sposobu obliczania ceny.

1. Wykonawca określa cenę realizacji zamówienia poprzez wskazanie w Formularzu ofertowym sporządzonym wg wzoru stanowiącego **Załącznik nr 2** do SIWZ ceny ofertowej netto i brutto za realizację przedmiotu zamówienia.
2. Cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia, zgodnie z opisem przedmiotu zamówienia oraz wzorem umowy określonym w niniejszej SIWZ.
3. Zamawiający **przewiduje** możliwość zmian ceny ofertowej brutto **jedynie** w przypadku zmiany stawki podatku od towarów i usług.
4. Ceny ofertowe muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).

5. Ceny ofertowe winne być wyrażone w złotych polskich (PLN).
6. Jeżeli w postępowaniu złożona zostanie oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. W takim przypadku Wykonawca, składając ofertę, jest zobligowany poinformować Zamawiającego w tej ofercie, że wybór jego oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę **(rodzaj) towaru**, którego **dostawa** będzie prowadzić do jego powstania oraz wskazując ich wartość bez kwoty podatku.

Rozdział XIII. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert.

1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie kierował się następującymi kryteriami (w nawiasie waga kryterium – maksymalna liczba punktów jaką może uzyskać oferta w danym kryterium):
   1) cena ofertowa (60 pkt);
   2) okres wsparcia opisany w pkt. 5 OPZ w miesiącach [minimum 24 miesięcy, wsparcie dłuższe niż 36 miesięcy będzie liczone jako 36-miesięczne] (25 pkt);
   3) czas dostawy w dniach [czas krótszy niż 15 dni będzie liczony jak 15 dni, maksimum 60 dni od dnia podpisania umowy] (15 pkt).

   Zamawiający udzieli zamówienia temu Wykonawcy, którego oferta otrzyma największą liczbę punktów, wyliczoną wg wzoru:

   $$\mathbf{P^{of}_n = (c^{of}_{min} / c^{of}_n \times 60\ pkt) + (ow^{of}_n / ow^{of}_{max} \times 25\ pkt) + (cd^{of}_{min} / cd^{of}_n \times 15\ pkt)}$$

   c^{of}_n – cena rozpatrywanej oferty,
   c^{of}_{min} – najniższa cena ze wszystkich złożonych ofert,
   ow^{of}_n – okres wsparcia rozpatrywanej oferty (wsparcie dłuższe niż 5-letnie będą oceniane jak 5-letnie)
   ow^{of}_{max} – najdłuższy okres wsparcia ze wszystkich złożonych ofert,
   cd^{of}_{min} – najkrótszy, deklarowany, ze wszystkich złożonych ofert czas dostawy,
   cd^{of}_n – czas deklarowany dostawy z rozpatrywanej oferty.

2. Punktacja przyznawana ofertom w poszczególnych kryteriach będzie liczona z dokładnością do dwóch miejsc po przecinku. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.
3. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w ustawie PZP oraz w SIWZ i zostanie oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru.
4. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert uzyskają taką samą liczbę punktów, Zamawiający spośród tych ofert dokona wyboru oferty z niższą ceną (art. 91 ust. 4 ustawy PZP).
5. Zamawiający nie przewiduje przeprowadzenia dogrywki w formie aukcji elektronicznej.

Rozdział XIV. Informacje o formalnościach, jakie powinny być dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

1. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
2. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający może żądać przed zawarciem umowy przedstawienia umowy regulującej współpracę tych Wykonawców. Umowa taka winna określać strony umowy, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdemu z nich, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania konsorcjum (obejmującego okres realizacji przedmiotu zamówienia, gwarancji i rękojmi), wykluczenie możliwości wypowiedzenia umowy konsorcjum przez któregokolwiek z jego członków do czasu wykonania zamówienia.

3. W wyniku postępowania zostanie zawarta umowa zgodna ze wzorem Zamawiającego.
4. Postanowienia ustalone we wzorze umowy nie podlegają negocjacjom.
5. W przypadku, gdy Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy, Zamawiający będzie mógł wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownego badania i oceny, chyba że zachodzą przesłanki, o których mowa w art. 93 ust. 1 ustawy PZP.

Rozdział XV. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

Rozdział XVI. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach.

Wzór umowy stanowi **Załącznik nr 3** do SIWZ.

Zamawiający przewiduje możliwość zmiany zapisów umowy zgodnie z art. 144 PZP w zakresie dostawy sprzętu o identycznych lub lepszych parametrach od zaoferowanych w ofercie, przy zachowaniu ceny ofertowej.

Rozdział XVII. Pouczenie o środkach ochrony prawnej.

1. Każdemu Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy PZP przysługują środki ochrony prawnej przewidziane w dziale VI ustawy PZP jak dla postępowań **powyżej** kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 ustawy PZP.
2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy PZP.

Rozdział XVIII. Inne informacje.

OCHRONA DANYCH OSOBOWYCH

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem danych osobowych przekazanych w złożonej ofercie będzie Sąd Najwyższy, 00-951 Warszawa, pl. Krasińskich 2/4/6, e-mail: iod@sn.pl;
  http://www.sn.pl/informacjepraktyczne/SitePages/Ochrona_danych_osobowych.aspx ;
- z Inspektorem Ochrony Danych Osobowych można się kontaktować pod adresem e-mail: iod@sn.pl;
- dane osobowe przekazane w złożonej ofercie będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego;
- odbiorcami danych osobowych przekazanych w złożonej ofercie będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa PZP";
- dane osobowe przekazane w złożonej ofercie będą przechowywane, zgodnie z art. 97 ust. 1 ustawy PZP, przez okres co najmniej 4 lat od dnia zakończenia postępowania o udzielenie zamówienia; jeżeli czas trwania umowy przekracza 4 lata, to okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania danych osobowych jest wymaganiem ustawowym określonym w przepisach ustawy PZP, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy PZP;

- w odniesieniu do danych osobowych przekazanych w złożonej ofercie decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
- osoba, której dane osobowe widnieją w dokumentach postępowania posiada:
  - na podstawie art. 15 RODO prawo dostępu do swoich danych osobowych;
  - na podstawie art. 16 RODO prawo do sprostowania swoich danych osobowych;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy osoba ta uzna, że przetwarzanie jej danych osobowych narusza przepisy RODO;
- nie przysługują osobie, której dane osobowe widnieją w dokumentach postępowania:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych w postępowaniu jest art. 6 ust. 1 lit. c RODO.

DYREKTOR
Biura Informatyki
w Sądzie Najwyższym
Maciej Pajączkowski

GŁÓWNY SPECJALISTA
d/s. Zamówień Publicznych
w Sądzie Najwyższym
dr inż. Jerzy Dyleweski

Załącznik nr 1 do SIWZ

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa urządzeń sieciowych:
- 5 szt. przełączników typ I,
- 2 szt. przełączników typ II,
- 1 szt. kontrolera sieci bezprzewodowej,
- 9 szt. punktów dostępowych sieci bezprzewodowej,

wraz z systemem zarządzania i monitoringu oraz wyposażeniem dodatkowym, mająca na celu modyfikację infrastruktury sieciowej do zmieniających się standardów w siedzibie Sądu Najwyższego.

W zmodyfikowanej infrastrukturze Zamawiający zamierza wykorzystywać posiadane już przez niego komponenty, stąd wymaganie, żeby oferowane urządzenia były kompatybilne z tymi komponentami, w szczególności z systemem Cisco Identity Services Engine 2.4 (ISE), przełącznikami Cisco Catalyst 3650, Cisco Catalyst 3750X, Cisco Catalyst 2960X, Cisco Catalyst 2960CX, Cisco Catalyst 3560CX, Cisco Catalyst 9300 z licencją DNA Essentials i DNA Premier, punktami dostępowymi Cisco Aironet 2800 oraz modułami światłowodowymi Cisco 10G LRM oraz Cisco 10G SR.

Rozwiązaniem równoważnym będzie zastąpienie komponentów infrastruktury sieciowej Zamawiającego niekompatybilnych z oferowanymi przez Wykonawcę produktami, przez dostarczenie i wdrożenie odpowiedników tych komponentów, kompatybilnych z zaoferowanymi rozwiązaniami. Wdrożenie rozwiązania równoważnego musi odbyć się w sposób nieutrudniający pracy sędziom i pracownikom Sądu Najwyższego, tj. od piątku od godziny 16:30 do niedzieli do godziny 23:30 (łącznie 55 godzin).

1. Ogólne wymagania odnośnie urządzeń

1.1. Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refurbished/odnowione (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).

1.2. Oferowane urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia producenta lub przedstawiciela producenta potwierdzającego ważność i zakres uprawnień licencyjnych.

1.3. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u producenta lub polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.

1.4. Wszystkie urządzenia i moduły muszą pochodzić od producenta dostarczanych urządzeń i muszą być objęte kontraktem serwisowym producenta, którym będą objęte dostarczane urządzenia.

2. Wymaganie kompatybilności dla wszystkich przełączników sieciowych

2.1 Oferowane przełączniki muszą znajdować się na liście kompatybilności producenta z posiadanym przez Zamawiającego systemem kontroli dostępu Cisco Identity Services Engine 2.4 w tabeli 2 „Supported Cisco Access Switches" oraz muszą zapewniać pełne wsparcie w zakresie wszystkich wymienionych w tej tabeli funkcjonalności, czyli: AAA, Profiling, BYOD, Guest, Guest Originating URL, Posture, MDM oraz TrustSec.
Lista kompatybilności dostępna jest na stronie:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/compatibility/b_ise_sdt_24.htm

3. Wymagania dla przełącznika sieciowego typ I (5 szt.):

3.1 Przełącznik musi być stackowalny oraz wyposażony w minimum 48 portów RJ-45 typu 10/100/1000Base-T.

3.2 Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z umożliwiajacy jego wymianę „na gorąco" (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne w ofercie producenta w chwili składania oferty co najmniej następujące moduły:

3.2.1 posiadajace z co najmniej 4 gniazda/porty SFP dla modułów interfejsów 1Gbps;
3.2.2 posiadajace z co najmniej 4 gniazda RJ-45 typu mGig (100Mbps, 1Gbps, 2,5Gbps, 5Gbps, 10Gbps);
3.2.3 posiadajace z co najmniej 8 gniazd /portów SFP/SFP+ dla modułów interfejsów 1/10Gbps;
3.2.4 posiadajace z co najmniej 2 gniazda /porty QSFP+ dla modułów interfejsów 40Gbps;
3.2.5 posiadajace z co najmniej 2 gniazda /porty SFP28 dla modułów interfejsów 25Gbps.

3.3 Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-BX.

3.4 Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH).

3.5 Porty QSFP+ muszą umożliwiać obsadzenie modułami 40G-SR, 40G-CSR, 40G-LR4 oraz 40G-ER4.

3.6 Przełączniki w momencie dostawy muszą być wyposażone w moduł posiadający 8 gniazd/portów na moduły SFP+ przeznaczone do instalacji modułów SFP+ o przepustowości 10Gbps.

3.7 Przełącznik musi zapewniać możliwość stackowania (łączenia w stos) z zapewnieniem następujących parametrów:
3.7.1 przepustowość w ramach stosu co najmniej 480Gb/s;
3.7.2 co najmniej 8 urządzeń w stosie;
3.7.3 stos widoczny jako jeden node dla procesu spanning-tree;
3.7.4 zarządzanie poprzez jeden adres IP;
3.7.5 możliwość tworzenia połączeń cross-stack link aggregation (tj. dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad.

3.8 Przełącznik musi umożliwiać współdzielenie mocy zasilaczy (łączenie w stos mocy, ang. power-stack) tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie mocy (tzw. redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie). Stos mocy musi umożliwiać połączenie co najmniej 4 przełączników.

3.9 Przełącznik musi być wyposażony w redundantne i wymienne moduły wentylatorów.

3.10 Przełącznik musi być zasilany prądem przemiennym 230V, musi posiadać możliwość instalacji zasilacza redundantnego. Zasilacz redundantny nie jest wymagany w tym postępowaniu. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne.

3.11 Przełącznik musi posiadać szybkość przełączania zapewniającą pracę z pełną wydajnością wszystkich interfejsów (256 Gbps) – również dla pakietów 64-bajtowych (przełącznik line-rate).

3.12 Przełącznik musi zapewniać wydajność przesyłania co najmniej 190 Mpps.

3.13 Przełącznik musi posiadać co najmniej 16MB bufor pamięci współdzielony przez wszystkie porty.

3.14 Przełącznik musi posiadać co najmniej 8GB pamięci DRAM i co najmniej 16GB pamięci flash.

3.15 Przełącznik musi sprzętowo zapewniać/osiągać/posiadać:
3.15.1 pojemność tablicy MAC dla co najmniej 32000 wpisów;
3.15.2 minimum 4000 VLAN ID;
3.15.3 obsługę ramek Ethernet o wielkości minimum 9198 bajtów (jumbo frames);
3.15.4 co najmniej 32000 wpisów dla hostów w tablicy routingu IPv4;
3.15.5 co najmniej 16000 wpisów dla hostów w tablicy routingu IPv6;
3.15.6 co najmniej 5000 wpisów w tablicy QoS;
3.15.7 co najmniej 5000 wpisów w tablicy ACL.

3.16 Przełącznik musi zapewniać /posiadać obsługę:
3.16.1 protokołu NTP;
3.16.2 IGMPv1/2/3;
3.16.3 protokołu IEEE 802.1ab LLDP i LLDP-MED.

3.17 Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
3.17.1 IEEE 802.1w Rapid Spanning Tree;
3.17.2 Per-VLAN Rapid Spanning Tree (PVRST+);
3.17.3 IEEE 802.1s Multi-Instance Spanning Tree;
3.17.4 obsługa co najmniej 128 instancji protokołu STP.

3.18 Przełącznik musi zapewniać obsługę funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
3.19 Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
3.20 Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
- 3.20.1 obsługę co najmniej 5 poziomów dostępu administracyjnego poprzez konsolę - przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level);
- 3.20.2 autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN;
- 3.20.3 autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
- 3.20.4 obsługę funkcji Guest VLAN umożliwiającą uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X;
- 3.20.5 możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
- 3.20.6 możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X;
- 3.20.7 mozliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem;
- 3.20.8 możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176;
- 3.20.9 obsługę funkcjonalności flexible authentication (tj. możliwość wyboru kolejności uwierzytelniania – 802.1X /uwierzytelnianie w oparciu o MAC adres /uwierzytelnianie w oparciu o portal www);
- 3.20.10 obsługę funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;
- 3.20.11 obsługę 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);
- 3.20.12 możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+;
- 3.20.13 obsługę list kontroli dostępu (ACL), z możliwością konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia).

3.21 Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
- 3.21.1 implementację co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi;
- 3.21.2 implementację algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek;
- 3.21.3 obsługę jednej z wyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority);
- 3.21.4 klasyfikację ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów:
  - 3.21.4.1 źródłowy/docelowy adres MAC,
  - 3.21.4.2 źródłowy/docelowy adres IP,
  - 3.21.4.3 źródłowy/docelowy port TCP;
- 3.21.5 ograniczanie dostępnego pasma na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting);
- 3.21.6 kontrolę sztormów dla ruchu broadcast/multicast/unicast;
- 3.21.7 możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

3.22 Przełącznik musi posiadać wbudowany analizator pakietów.
3.23 Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7).
3.24 Przełącznik musi umożliwiać szyfrowanie w standardzie IEEE 802.1AE (szyfrowanie ruchu) 256-bit z prędkością linerate dla każdego z interfejsów.

3.25 Przełącznik musi zapewniać obsługę współpracy z systemami umożliwiającymi wykrywanie zagrożeń w ruchu zaszyfrowanym w oparciu o rozszerzone informacje Netflow.
3.26 System operacyjny przełącznika musi być konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz umożliwiać eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
3.27 Przełącznik musi umożliwiać uruchamianie zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia.
3.28 Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).
3.29 Przełącznik musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 60000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.
3.30 Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
3.31 Przełącznik musi posiadać dedykowany port Ethernet do zarządzania out-of-band.
3.32 Przełącznik musi posiadać co najmniej jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych oraz umożliwiać uruchomienie z nośnika danych umieszczonego w porcie USB.
3.33 Przełącznik musi być wyposażony w port konsoli USB.
3.34 Plik konfiguracyjny przełącznika musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
3.35 Przełącznik musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
3.36 Przełącznik musi umożliwiać zdalną obserwację 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).
3.37 Przełącznik musi umożliwiać obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
3.38 Przełącznik musi posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
3.39 Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.
3.40 Przełącznik musi być być kompatybilny z posiadanymi przez Zamawiającego modułami światłowodowymi Cisco SFP-10G-LRM= (ma umożliwiać wykorzystanie tych modułów w portach SFP+ przełącznika).
3.41 Przełącznik musi umożliwiać instalację w szafie RACK 19'' i zajmować w niej nie więcej niż 1U – do każdego przełącznika należy dostarczyć zestaw montażowy.
3.42 Jeżeli jakieś funkcjonalności wymagają zakupu licencji lub subskrypcji czasowych, należy je zapewnić na okres 36 miesięcy.
3.43 Wraz z przełącznikiem należy dostarczyć 50 sztuk licencji ISE Base oraz 50 szt. licencji ISE Plus na 36 miesięcy do systemu kontroli dostępu Cisco Identity Services Engine (ISE) 2.4 używanego przez Zamawiającego.

4 Wymagania dla przełącznika sieciowego typ II (2 szt.):
4.1 Przełącznik musi być wyposażony w 24 porty 10/100/1000BaseT RJ-45 oraz 4 porty uplink 1G SFP
4.2 Porty SFP muszą umożliwiać ich obsadzenie następującymi rodzajami wkładek:
4.2.1 Gigabit Ethernet 1000Base-T,
4.2.2 Gigabit Ethernet 1000Base-SX,
4.2.3 Gigabit Ethernet 1000Base-LX/LH,
4.2.4 Gigabit Ethernet 1000Base-EX,

4.2.5 Gigabit Ethernet 1000Base-ZX,
4.2.6 Gigabit Ethernet 1000Base-BX-D/U

4.3 Przełącznik musi zapewniać możliwość stackowania (łączenia w stos) z zapewnieniem następujących parametrów:
4.3.1 przepustowość w ramach stosu - 80Gb/s,
4.3.2 8 urządzeń w stosie,
4.3.3 zarządzanie poprzez jeden adres IP,
4.3.4 możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
4.3.5 jeżeli stackowanie jest realizowane za pomocą modułu instalowanego w przełączniku, należy go dostarczyć w tym postępowaniu

4.4 Zasilanie i chłodzenie:
4.4.1 przełącznik musi być zasilany prądem przemiennym 230V, musi posiadać możliwość instalacji zasilacza redundantnego. Zasilacz redundantny nie jest wymagany w tym postępowaniu. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne.
4.4.2 przełącznik musi posiadać redundantne wentylatory,

4.5 Przepustowość przełącznika (switching capacity) 56 Gb/s (bez podłączenia do stosu), 136 Gb/s (z podłączeniem do stosu)

4.6 Prędkość przesyłania (forwarding rate) 41.66 Mpps

4.7 Bufor pakietów – 6MB

4.8 Pamięć DRAM – 2GB

4.9 Pamięć flash – 4GB

4.10 Przełącznik musi:
4.10.1 zapewniać obsługę 500 aktywnych sieci VLAN;
4.10.2 zapewniać obsługę 16000 adresów MAC;
4.10.3 zapewniać obsługę 3000 tras IPv4;
4.10.4 zapewniać obsługę 1500 tras IPv6;
4.10.5 umożliwiać ilość wpisów w listach kontroli dostępu Security ACL – 1000;
4.10.6 umożliwiać ilość wpisów w listach kontroli dostępu QoS ACL – 1000;
4.10.7 zapewniać obsługę 512 interfejsów SVI L3;
4.10.8 zapewniać obsługę Jumbo frame 9198B;
4.10.9 zapewniać obsługę 48 połączeń zagregowanych typu „port channel”;
4.10.10 zapewniać obsługę 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.

4.11 Przełącznik musi obsługiwać protokół NTP.

4.12 Przełącznik musi obsługiwać IGMPv1/2/3 i MLDv1/2 Snooping.

4.13 Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
4.13.1 IEEE 802.1w Rapid Spanning Tree;
4.13.2 Per-VLAN Rapid Spanning Tree (PVRST+);
4.13.3 IEEE 802.1s Multi-Instance Spanning Tree;
4.13.4 Obsługa 64 instancji protokołu STP.

4.14 Przełącznik musi obsługiwać protokoły LLDP i LLDP-MED.

4.15 Przełącznik musi posiadać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.

4.16 Przełącznik musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego.

4.17 Przełącznik musi umożliwiać uruchomienie funkcji serwera DHCP.

4.18 Przełącznik musi posiadać mechanizmy związane z bezpieczeństwem sieci:
4.18.1 obsługę wielu poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level);

4.18.2 autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN;
4.18.3 autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL;
4.18.4 obsługę funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X;
4.18.5 umożliwiać uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
4.18.6 umożliwiać uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X;
4.18.7 umożliwiać uwierzytelnianie wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem;
4.18.8 umożliwiać obsługę żądań Change of Authorization (CoA) zgodnie z RFC 5176;
4.18.9 posiadać funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www);
4.18.10 umożliwiać obsługę funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;
4.18.11 zapewnieniać podstawowe mechanizmy 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);
4.18.12 umożliwiać autoryzację prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+;
4.18.13 umożliwiać obsługę list kontroli dostępu (ACL) następujących typów:
4.18.13.1 port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika;
4.18.13.2 VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika;
4.18.13.3 Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
4.18.13.4 umożliwiać konfigurację tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
4.18.14 umożliwiać szyfrowanie ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA);
4.18.15 posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing);
4.18.16 Funkcja Private VLAN.
4.19 Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
4.19.1 sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
4.19.2 bezpieczna sekwencja uruchamiania,
4.19.3 sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
4.20 Przełącznik musi posiadać mechanizmy związane z zapewnieniem jakości usług w sieci:
4.20.1 implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi;
4.20.2 implementację algorytmu Shaped Round Robin dla obsługi kolejek;
4.20.3 umożliwiać obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority);
4.20.4 umożliwiać klasyfikację ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów:
4.20.4.1 źródłowy/docelowy adres MAC,

4.20.4.2 źródłowy/docelowy adres IP,
4.20.4.3 źródłowy/docelowy port TCP;
4.20.5 umożliwiać ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
4.20.6 posiadać kontrolęa sztormów dla ruchu broadcast/multicast/unicast,
4.20.7 umożliwiać zmianę przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

4.21 Obsługa protokołów i mechanizmów routingu:
4.21.1 routing statyczny dla IPv4 i IPv6,
4.21.2 routing dynamiczny – RIP, OSPF do 1000 tras, PIM Stub do 1000 tras
4.21.3 policy-based routing (PBR),
4.21.4 umożliwiać obsługę protokołu redundancji bramy (VRRP) z obsługą 64 grup,
4.21.5 umożliwiać obsługę 10 tuneli GRE (Generic Routing Encapsulation);

4.22 Przełącznik misi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN.

4.23 Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).

4.24 Przełącznik musi posiadać funkcjonalność sondy IP SLA Responder.

4.25 Zarządzanie:
4.25.1 przełącznik musi posiadać port konsoli;
4.25.2 przełącznik musi posiadać dedykowany port Ethernet do zarządzania out-of-band;
4.25.3 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 w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją;
4.25.4 przełącznik musi umożliwiać obsługę protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
4.25.5 przełącznik musi umożliwiać konfigurację za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów;
4.25.6 przełącznik musi wsperać protokół RESTCONF;
4.25.7 przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
4.25.8 przełącznik musi posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
4.25.9 przełącznik musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Przełącznik musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
4.25.10 przełącznik musi posiadać wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;

4.26 Przełącznik musi umożliwiać instalację w szafie RACK 19'' i zajmować w niej nie więcej niż 1U – do każdego przełącznika należy dostarczyć zestaw montażowy.

4.27 Przełącznik musi umożliwiać próbkowanie (bez samplowania) i eksportowanbie statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow).

4.28 Przełącznik musi umożliwiać realizację rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.

4.29 Przełącznik musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.

4.30 Jeżeli jakieś funkcjonalności wymagają zakupu licencji lub subskrypcji czasowych, należy je zapewnić na okres 36 miesięcy.

5 Wymagania dla Kontrolera sieci bezprzewodowej (1 szt.):

5.1 Kontroler sieci bezprzewodowej ma być uruchamiany w formie maszyny wirtualnej m.in. w środowisku VMware posiadanym przez Zamawiającego, umożliwiając centralną kontrolę punktów dostępu bezprzewodowego zgodnie z protokołem CAPWAP (RFC 5415) i zapewniając co najmniej:

5.1.1 zarządzanie politykami bezpieczeństwa;

5.1.2 wykrywanie zagrożeń w sieci bezprzewodowej;

5.1.3 zarządzanie pasmem radiowym;

5.1.4 zarządzanie mobilnością;

5.1.5 zarządzanie jakością transmisji.

5.2 Kontroler sieci bezprzewodowej musi obsługiwać do 6000 punktów dostępowych w zależności od platformy, na której zainstalowano oprogramowanie

5.3 Kontroler sieci bezprzewodowej musi obsługiwać do 10000 klientów sieci bezprzewodowej w zależności od platformy, na której zainstalowano oprogramowanie

5.4 Kontroler sieci bezprzewodowej musi wspierać chmury i platformy wirtualne: AWS (Amazon Web Services), GCP (Google Cloud Platform), ESXi, KVM, Hyper-V

5.5 Kontroler sieci bezprzewodowej musi umożliwiać zapewnienia wysokiej dostępności (HA) platformy przez zastosowanie następujących mechanizmów (w przypadku zakupienia dodatkowej licencji w przyszłości):

5.5.1 dla ESXi i KVM: SSO (Stateful Switchover), N+1

5.5.2 dla AWS i GCP: N+1

5.6 Kontroler sieci bezprzewodowej musi obsługiwać wydajność centralnego przełączania ruchu 1,5 Gbps (dotyczy chmury prywatnej i platform ESXi oraz KVM)

5.7 Kontroler sieci bezprzewodowej musi obsługiwać zarządzanie pasmem radiowym punktów dostępowych:

5.7.1 automatyczna adaptacja do zmian w czasie rzeczywistym;

5.7.2 optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia);

5.7.3 dynamiczne przydzielanie kanałów radiowych;

5.7.4 wykrywanie, eliminacja i unikanie interferencji;

5.7.5 równoważenie obciążenia punktów dostępowych;

5.7.6 tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych;

5.7.7 automatyczna dystrybucja klientów pomiędzy punkty dostępowe;

5.7.8 mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych;

5.7.9 dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe.

5.8 Kontroler sieci bezprzewodowej musi umożliwiać mapowanie SSID do segmentów VLAN w sieci przewodowej:

5.8.1 1:1;

5.8.2 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty);

5.8.3 możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID).

5.9 Kontroler sieci bezprzewodowej musi obsługiwać sieci kratowe zapewniając:

5.9.1 komunikacjęa między punktami dostępowymi bez medium kablowego;

5.9.2 separację trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi);

5.9.3 automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo);

5.9.4 automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji);

5.9.5 autoryzację punktów dostępowych w oparciu o certyfikaty, adresy MAC;

5.10 Kontroler sieci bezprzewodowej musi obsługiwać mechanizmy bezpieczeństwa:

5.10.1 802.11i, WPA3, WPA2, WPA, WEP;
5.10.2 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST);
5.10.3 serwery autoryzacyjne – RADIUS, TACACS+, z wbudowaną lokalna baza użytkowników;
5.10.4 kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID;
5.10.5 obsługę profilowania użytkowników:
5.10.5.1 przydział sieci VLAN,
5.10.5.2 przydział list kontroli dostępu (ACL);
5.10.6 uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w;
5.10.7 uwierzytelnianie punktów dostępowych w oparciu o certyfikaty;
5.10.8 obsługę list kontroli dostępu (ACL);
5.10.9 obsługę indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X;
5.10.10 wykrywanie i dezaktywację obcych punktów dostępowych;
5.10.11 ochronę kryptograficzną (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP;
5.10.12 eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa);
5.10.13 posiadć zabezpieczenia zapewniające autentyczność oprogramowania i firmware'u:
5.10.13.1 kryptograficzne podpisywanie obrazów oprogramowania, BIOS i innego oprogramowania wchodzącego w skład kontrolera,
5.10.13.2 bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych;
5.11 Obsługę ruchu unicast IPv4 i IPv6.
5.12 Obsługę ruchu multicast IPv4 i IPv6:
5.12.1 IGMP / MLD snooping;
5.12.2 optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym;)
5.12.3 obsługa konwersji ruchu multicast do unicast.
5.13 Obsługę mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami).
5.14 Obsługę mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k.
5.15 Wsparcie dla IEEE 802.11u.
5.16 Obsługę mechanizmów QoS:
5.16.1 802.1p;
5.16.2 WMM, TSpec, U-APSD;
5.16.3 Ograniczanie pasma per użytkownik;
5.16.4 Call Admission Control, SIP CAC, Call Snooping;
5.16.5 równomierną obsługę klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego (również w trybie mesh);
5.16.6 kontrolę przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID.
5.17 Obsługę sensorów symulujących pracę klientów bezprzewodowych, które pozwalają na badanie działania wybranych usług w sieci (DNS, DHCP, RADIUS, IMAP, Outlook Web Access, inne) i eksportują wyniki testów do dedykowanego zewnętrznego kolektora.
5.18 Obsługę mechanizmów wysokiej dostępności, takich jak możliwość wgrania łatki oprogramowania bez restartu koncentratora (hot patching), restartu danego procesu, odseparowania systemów operacyjnych punktów dostępowych od systemu kontrolera, sekwencyjnego uaktualniania oprogramowania punktów dostępowych (rolling upgrades).
5.19 Obsługę enkapsulacji ruchu VXLAN.
5.20 Obsługę dostępu gościnnego (IPv4 i IPv6):
5.20.1 przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony);
5.20.2 przekierowanie użytkowników do strony logowania na zewnętrznym serwerze.
5.21 Współpracować z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługiwać tagi telemetryczne.
5.22 Obsługę NTP wersji 4 (IPv4 oraz IPv6)

5.23 Umożliwiać definiowanie polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania.
5.24 Obsługę Hotspot 2.0.
5.25 Obsługę redundancji 1:1 (active/standby) zapewniającą (w przypadku zakupienia dodatkowej licencji w przyszłości):
  5.25.1 utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera,
  5.25.2 synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej.
5.26 Analizę ruchu pozwalającą na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7), obsługę znakowania, limitowania lub odrzucania ruchu; rozpoznawania ponad 1400 aplikacji na podstawie sygnatur oraz ponad 150 aplikacji enkryptowanych.
5.27 Zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow.
5.28 Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji.
5.29 Obsługę protokołu Bonjour poprzez wbudowany mDNS Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów.
5.30 Zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej.
5.31 Obsługę wbudowanego interpretera języka PYTHON.
5.32 Obsługę API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020).
5.33 Posiada wbudowanę bazę najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem.
5.34 Kontroler musi być kompatybilny z posiadanym przez Zamawiającego systemem kontroli dostępu Cisco Identity Services Engine (ISE) 2.4 – musi znajdować się na liście kompatybilności dostępnej pod adresem https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/compatibility/b_ise_sdt_24.html
5.35 Wraz z kontrolerem należy dostarczyć licencje na obsługę dostarczanych w tym postępowaniu punktów dostępowych oraz dla siedmiu punktów dostępowych Cisco Aironet 2800 (AIR-AP2802I-E-K9) posiadanych przez Zamawiającego. Jeżeli są to licencje czasowe muszą zostać dostarczone na 36 miesięcy. Licencje muszą umożliwiać wykorzystanie pełnej funkcjonalności oferowanej przez kontroler dla danego typu punktów dostępowych.

6 Wymagania dla punktu dostępowego sieci bezprzewodowej (9 szt.):
6.1 Punkt dostępowy musi być w pełni kompatybilny z opisanym w punkcie 5 kontrolerem sieci bezprzewodowej.
6.2 Punkt dostępowy musi obsługiwać standardy 802.11a/b/g/n/ac/ax obejmujace obslugę:
  6.2.1 OFDMA (uplink/downlink), TWT, BSS Coloring;
  6.2.2 MU-MIMO – min. 4x4:4;
  6.2.3 20 kanałów, 40 MHz dla 802.11n
  6.2.4 20 kanałów, 40, 80, 160 MHz dla 802.11ac/ax
  6.2.5 prędkości PHY do 3,47 Gbps (ac)
  6.2.6 prędkośći PHY do 5,38 Gbps (ax)
  6.2.7 agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
  6.2.8 beamforming dla klientów 802.11a/g/n/ac/ax
  6.2.9 MRC (Maximal Ratio Combining)
6.3 Punkt dostępowy musi obsługiwać szerokiego zakresu kanałów radiowych:
  6.3.1 min. 13 kanałów dla zakresu 2.4 GHz;
  6.3.2 min. 8 kanałów dla zakresu 5GHz (UNII-1 i UNII-2);
  6.3.3 min. 8 kanałów dla zakresu 5GHz (extended UNII-2).
6.4 Punkt dostępowy musi posiadać konfigurowalną moc nadajnika:
  6.4.1 dla zakresu 2.4 GHz: do 100 mW;
  6.4.2 dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW;
  6.4.3 dla zakresu 5GHz (extended UNII-2): do 200 mW.
6.5 Punkt dostępowy musi posiadać możliwość zmiany trybu pracy modułów radiowych (elastyczna praca drugiego modułu):

6.5.1 jeden moduł pracujący w paśmie 2,4GHz, drugi moduł pracujący w paśmie 5GHz;
6.5.2 oba moduły pracujące w paśmie 5GHz na różnych kanałach w celu wytworzenia mikro i makro komórki radiowej.

6.6 Punkt dostępowy musi być zgodny z protokołem CAPWAP (RFC 5415) i umożliwiać zarządzanie przez kontroler WLAN z funkcjonalnościami:
6.6.1 automatycznego wykrywania kontrolera i konfiguracji poprzez sieć LAN;
6.6.2 optymalizacji wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany);
6.6.3 obsługi min. 16 BSSID;
6.6.4 definiowania polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID;
6.6.5 uwierzytelniania ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w;
6.6.6 obsługi trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN);
6.6.7 możliwości pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników;
6.6.8 obsługi tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6;
6.6.9 jednoczesnej obsługi transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS);
6.6.10 obsługi Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h;
6.6.11 obsługi IPv6;
6.6.12 obsługi szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r;
6.6.13 obsługi mechanizmów QoS:
6.6.13.1 ograniczania ruchu do użytkownika, z możliwością konfiguracji per użytkownik,
6.6.13.2 obsługi WMM, TSPEC, U-APSD;
6.6.14 współpracy z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne;
6.6.15 wsparciem dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
6.6.16 wsparciem IEEE 802.11i, WPA3, WPA2, WPA
6.6.17 wbudowany suplikant 802.1X – musi umożliwiać uwierzytelnianie AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP).

6.7 Punkt dostępowy musi mieć możliwość pracy jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach (zmiana trybu pracy, przez wgranie oprogramowania, musi być bezkosztowa w okresie trwania kontraktu serwisowego):
6.7.1 obsługa do 100 punktów dostępowych
6.7.2 obsługa do 2000 klientów
6.7.3 możliwość konfiguracji do 16 sieci bezprzewodowych
6.7.4 centralna optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
6.7.5 obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
6.7.6 obsługa mechanizmów wsparcia roamingu – IEEE 802.11k, IEEE 802.11v
6.7.7 jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)
6.7.8 wykrywanie do 1000 obcych klientów oraz do 100 obcych AP
6.7.9 konfiguracja polityk bezpieczeństwa per SSID
6.7.10 obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS)
6.7.11 współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
6.7.12 tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe
6.7.13 filtrowanie MAC adresów (Whitelist)
6.7.14 analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)

6.7.15 dwukierunkowe limitowanie transmisji (bidirectional rate-limiting ruchu) per klient, per WLAN, per BSSID
6.7.16 profilowanie (rozpoznawanie typów) urządzeń podłączających się do sieci bezprzewodowej
6.7.17 obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC)
6.7.18 obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym
6.7.19 obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta;
6.7.20 zarządzanie przez HTTPS
6.7.21 wsparcie SSH, SNMP, NTP, SYSLOG
6.7.22 obsługa aktualizacji oprogramowania przez SFTP
6.7.23 wbudowany serwer DHCP
6.7.24 wbudowany mechanizm redundancji automatycznie wybierający kontroler zapasowy wśród grupy obsługiwanych punktów dostępowych mogących pełnić funkcję kontrolera

6.8 Punkt dostępowy musi posiadać zintegrowany moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz) zapewniający:
6.8.1 dokładność analizy (kwant próbkowania) max. 200 kHz,
6.8.2 zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych,
6.8.3 automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.),
6.8.4 współpracę z mechanizmami optymalizacji wykorzystania pasma radiowego,
6.8.5 interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz.

6.9 Punkt dostępowy musi posiadać interfejs konsoli RJ45.
6.10 Punkt dostępowy musi posiadać port USB 2.0.
6.11 Punkt dostępowy musi posiadać 2 GB RAM, 1 GB Flash.
6.12 Punkt dostępowy musi posiadać pełną funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at), możliwość uruchomienia AP z wykorzystaniem PoE (802.3af).
6.13 Punkt dostępowy musi posiadać anteny zintegrowane o zysku:
6.13.1 dla modułu umożliwiającego pracę w obu pasmach: min. 4 dBi dla pasma 2,4 GHz oraz 5 dBi dla pasma 5 GHz;
6.13.2 dla dedykowanego modułu 5 GHz: min. 4 dBi.
6.14 Punkt dostępowy musi posiadać obudowę przystosowana do pracy w zakresie temperatur -20 – 50 st. C.
6.15 Punkt dostępowy musi posiadać diodową sygnalizację stanu urządzenia z możliwością deaktywacji.
6.16 Punkt dostępowy musi posiadać certyfikację WiFi Alliance: 802.11 a/b/g/n/ac, WMM, Passpoint.
6.17 Punkt dostępowy musi posiadać wbudowane radio Bluetooth Low Energy (BLE) 5.0.
6.18 Punkt dostępowy musi być IoT ready (Zigbee, Thread)
6.19 Punkt dostępowy musi umożliwiać uruchamianie aplikacji w kontenerach dostępnych bezpośrednio na AP.
6.20 Razem z punktem dostępowym musi zostać dostarczony power injector 802.3at

7 Wymagania dla serwera zarządzającego i monitorującego (1 szt.):
7.1 Serwer musi posiadać graficzny system do zarządzania i monitorowania sieci kampusowej przewodowej oraz bezprzewodowej.
7.2 Serwer musi posiadać funkcjonalności podstawowe z zakresu monitoringu sieci:
7.2.1 zbieranie i zapamiętywanie do 7 dni wstecz danych telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji z różnych źródeł danych: SNMP, Syslog, NetFlow, sensory bezprzewodowe WiFi;
7.2.2 analizy i korelacji danych telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji na podstawie różnych źródeł danych: SNMP, Syslog, NetFlow, sensory bezprzewodowe WiFi;

7.2.3 wyznaczenia na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu;

7.2.4 wizualizacji topologii sieci wraz połączeniami oraz wizualizacją indeksu jakości pracy danego monitorowanego obiektu;

7.2.5 wyznaczania i wizualizacji indeksów jakości pracy dla grup urządzeń sieciowych wg.:

7.2.5.1 typów urządzeń: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, kontroler WLAN, radiowy punkt dostępowy - w przedziałach czasowych ostatnie 7 dni, ostatnie 24h, ostatnie 3h, zadany przedział czasowy w okresie ostatnich 7 dni,

7.2.5.2 lokalizacji geograficznych;

7.2.6 wizualizacji na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych;

7.2.7 wyznaczania i wizualizacja indeksów jakości pracy dla grup użytkowników z rozbiciem na użytkowników przewodowych oraz bezprzewodowych wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup użytkowników;

7.2.8 prezentacji dla użytkowników przewodowych szczegółowych informacji o ilości użytkowników podłączonych do sieci oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci z podaniem typowych przyczyn braku podłączenia np.: problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np.: użytkownicy z problemem z usługą DHCP;

7.2.9 prezentacji dla użytkowników bezprzewodowych szczegółowej informacje o ilości użytkowników podłączonych do sieci z rozbiciem na grupy użytkowników o dobrej jakości i złej jakości pracy oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci bezprzewodowej z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej. Szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP;

7.2.10 generowania automatycznych komunikatów o stwierdzonych nieprawidłowościach w pracy sieci w oparciu o skorelowane informacje zbierane przez system z urządzeń sieciowych wraz z sugestią przyczyny, sposobu rozwiązania problemu oraz dalszych kroków diagnostycznych dla poszczególnych urządzeń sieciowych;

7.2.11 narzędzi do śledzenia ścieżki sieciowej dla danego ruchu w sieci np. w relacji pomiędzy dwoma hostami wraz podanie informacji o wszystkich węzłach na ścieżce, ich indeksie jakości pracy, topologii fizycznej i logicznej np. zaznaczenie tunelowania ruchu bezprzewodowego, dokładną informacją o interfejsach, przez który płynie ruch, z zaznaczeniem lokalizacji list ACL, które dokonują filtracji danego ruchu;

7.3 Serwer musi umożliwiać wykrywanie i analizę problemów w sieci poprzez:

7.3.1 automatyczną analizę zdarzeń w sieci oraz identyfikację i wyświetlanie na tej podstawie problemów w działaniu sieci na poziomie całej sieci lub poszczególnych monitorowanych obiektów np. problemy związane z danym urządzeniem, użytkownikiem lub aplikacją;

7.3.2 automatyczną priorytetyzację problemów;

7.3.3 dla danego problemu, podanie opisu problemu, dostarczenie informacji kontekstowej umożliwiającej identyfikację i rozwiązanie problemu, określenie lokalizacji, urządzeń oraz użytkowników dotkniętych problemem, propozycja sugerowanych działań umożliwiających rozwiązanie problemu wraz z możliwością dostępu do urządzeń sieciowych w celu natychmiastowego dostarczenia danych diagnostycznych.

7.4 Serwer musi umożliwiać monitoring urządzeń:

7.4.1 dla poszczególnych urządzeń sieciowych: dostępności i osiągalności;

7.4.2 w zakresie sieci bezprzewodowej wykresy:

7.4.2.1 ilości aktywnych i nieaktywnych punktów radiowych z podaniem dokładnej listy urządzeń w każdej z kategorii,

7.4.2.2 listy radiowych punktów dostępowych wg. ilości podłączonych klientów bezprzewodowych,
7.4.2.3 listy radiowych punktów dostępowych wg. poziomu zakłóceń i interferencji w funkcji pasma transmisji 2.4 GHz, 5 GHz.

7.5 Serwer musi umożliwiać eksport danych w postaci pliku csv pełnej listy wszystkich monitorowanych urządzeń sieciowych w całej sieci lub w danej domenie lub lokalizacji z podaniem modelu urządzenia, wersji systemu operacyjnego, adresu IP, indeksu jakości pracy, osiągalności, ilości zidentyfikowanych problemów, lokalizacji geograficznej.

7.6 Serwer musi umożliwiać łatwe filtrowanie listy urządzeń wg. kryteriów:
7.6.1 typ urządzenia: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, radiowy punkt dostępowy, kontroler WLAN;
7.6.2 stan jakości pracy urządzenia: jakość niska, średnia, wysoka;
7.6.3 lokalizacja;
7.6.4 model urządzenia;
7.6.5 wersja systemu operacyjnego;
7.6.6 adres IP.

7.7 Serwer musi zapewniać szczegółowy monitoring każdego z urządzeń sieciowych obejmujący:
7.7.1 wykres zmian indeksu jakości pracy urządzenia w zadanym okresie czasu do 7 dni wstecz;
7.7.2 szczegółową informację o następujących parametrach pracy urządzenia w dowolnym momencie pracy urządzenia do 7 dni wstecz; monitorowane parametry: utylizacja pamięci, utylizacja CPU, dostępność łączy uplinkowych (w górę sieci), poziom błędów na linkach, skojarzone zdarzenia zarejestrowane w systemie;
7.7.3 szczegółową listę problemów skojarzonych z danym urządzeniem bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz);
7.7.4 schemat topologii sieci, w której znajduje się dane urządzenie;
7.7.5 dostęp do zarejestrowanych w systemie zdarzeń związanych z danym urządzeniem z możliwością filtrowanie wg. ważności;
7.7.6 możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca (adresu IP);
7.7.7 możliwość bezpośredniego dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu z poziomu konsoli graficznej systemu zarządzania i monitorowania;
7.7.8 szczegółowe informacje o urządzeniu obejmujące:
7.7.8.1 wykres czasowy utylizacji CPU,
7.7.8.2 wykres czasowy utylizacji pamięci,
7.7.8.3 wykres czasowy dostępności urządzenia,
7.7.8.4 wykres czasowy temperatury urządzenia,
7.7.8.5 informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, numer skonfigurowanej sieci VLAN, MAC adresu podłączonego urządzenia, prędkość linku, FDX/HDX,
7.7.8.6 dla każdego z monitorowanych interfejsów informacje o:
7.7.8.6.1 wykres czasowy dostępności interfejsu,
7.7.8.6.2 wykres czasowy utylizacji interfejsu niezależnie w kierunku nadawczym i odbiorczym,
7.7.8.6.3 wykres czasowy poziomu błędów niezależnie w kierunku nadawczym i odbiorczym;
7.7.8.7 w przypadku urządzeń pracujących jako urządzenia w sieci SDN typu Network Fabric szczegółowe informacje na temat stanu połączenia z siecią podkładową, stanu podłączenia do systemu kontroli dostępu w sieci Network Fabric;

7.8 Serwer musi umożliwiać monitoring użytkowników obejmujący:
7.8.1 szczegółowe informacje o użytkowniku końcowym i urządzeniach, na których pracuje, takie jak:
7.8.1.1 identyfikator użytkownika,

7.8.1.2 nazwa hosta lub hostów,
7.8.1.3 adres MAC hosta lub hostów,
7.8.1.4 adres IPv4 i IPv6 hosta lub hostów,
7.8.1.5 typ urządzenia,
7.8.1.6 przełącznik lub punkt dostępowy, do którego jest podłączone dane urządzenie końcowe wykorzystywane przez użytkownika,
7.8.1.7 lokalizacja geograficzna;

7.8.2 wykres zmian indeksu jakości pracy użytkownika i urządzenia, urządzenia, które wykorzystuje w zadanym okresie czasu do 7 dni wstecz;

7.8.3 szczegółową informację o następujących parametrach pracy urządzenia końcowego wykorzystywanego przez użytkownika w dowolnym momencie do 7 dni wstecz. Monitorowane parametry: stan podłączenia do sieci, dla urządzeń bezprzewodowych: poziom sygnału RSSI, poziom szumów SNR, przepustowość połączenia, ilość danych otrzymanych i nadawanych, SSID sieci, do której jest podłączone urządzenie końcowe, nazwa radiowego punktu dostępowego, wykorzystywany kanał radiowy i pasmo.

7.8.4 szczegółową listę wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem końcowym;

7.8.5 schemat topologii sieci z zaznaczeniem urządzenia dostępowego do którego jest podłączony dane urządzenie końcowe;

7.8.6 dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzeniem z możliwością filtrowanie wg. ważności;

7.8.7 możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia (przełącznika / punktu dostępowego) do danego innego miejsca (adresu IP);

7.8.8 informacje o generowanym ruchu sieciowym przez użytkownika na danym urządzeniu końcowym z podziałem na aplikacje biznesowe oraz niebiznesowe. Szczegółowe informacje dla każdej z aplikacji takie jak: nazwa aplikacji, indeks jakości działania aplikacji w sieci, ilość ruchu (w bajtach), średnia przepustowość (w bps), parametry QoS faktyczne oraz oczekiwane, straty pakietów (maksymalne i średnie), opóźnienie sieciowe (maksymalne i średnie), jitter (maksymalny i średni);

7.8.9 szczegółowe informacje o urządzeniu końcowym wykorzystywanym przez użytkownika obejmujace:
7.8.9.1 wykres czasowy ilości danych nadawanych i otrzymywanych,
7.8.9.2 wykres czasowy ilości generowanych zapytań DNS i otrzymywanych odpowiedzi,
7.8.9.3 dla urządzeń bezprzewodowych wykres czasowy zmian wartości mocy sygnału radiowego RSSI oraz zmian wartości poziomu szumów SNR,
7.8.9.4 dodatkowe dane analityczne dla użytkowników urządzeń końcowych wyposażonych w system operacyjny Apple iOS.

7.9 Serwer musi umożliwiać monitoring aplikacji obejmujacy:

7.9.1 szczegółowe informacje o aplikacjach wykorzystywanych w sieci, takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego oraz wykrytych problemów związanych z daną aplikacją;

7.9.2 szczegółowe wykresy czasowe parametrów działania każdej z aplikacji z uwzględnieniem: przepustowości wykorzystywanej przez daną aplikację, strat pakietów, jitter, opóźnienia sieciowego, opóźnienia sieciowego po stronie klienta, opóźnienia sieciowego po stronie serwera, opóźnienia generowanego przez serwer aplikacyjny;

7.9.3 szczegółowa lista wszystkich użytkowników wykorzysujących daną aplikację w sieci z podaniem urządzenia końcowego, które wykorzystuje daną aplikację.

7.10 Serwer musi umożliwiać monitoring sieci bezprzewodowej:

7.10.1 wizualizację graficzną rozmieszczenia poszczególnych radiowych punktów dostępowych, sensorów, oraz klientów sieci bezprzewodowej na mapie budynku;

7.10.2 graficzne planowanie i zarządzanie siecią bezprzewodową (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków;

7.10.3 monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych;
7.10.4 współpracę z systemami lokalizacji urządzeń radiowych (punktów dostępowych, klientów, tagów) z prezentacją graficzną na mapie;
7.10.5 narzędzie pozwalające na wykonywanie testów poprawności pracy sieci bezprzewodowej poprzez generowanie syntetycznego ruchu przez punkty dostępowe lub dedykowane sensory bezprzewodowe pozwalające na badanie/wykonanie testu:
7.10.5.1 czasu podłączania się do sieci: asocjacja, uwierzytelnienie, adresacja z DHCP,
7.10.5.2 pracy usług: DNS, RADIUS, dostępność bramy, dostępność określonych adresów IP,
7.10.5.3 pracy aplikacji: POP3, IMAP, Outlook Web Access, FTP, HTTP, HTTPS,
7.10.5.4 możliwość określenia czasu lub częstotliwości wykonywania testów;
7.10.6 narzędzie pozwalające na zbieranie od urządzeń Apple informacji o:
7.10.6.1 typie urządzenia i wersji oprogramowania;
7.10.6.2 parametrach pracy sieci bezprzewodowej z perspektywy urządzenia (słyszane punkty bezprzewodowe oraz ich parametry pracy);
7.10.6.3 przyczynie ostatniego rozłączenia/przełączenia z siecią bezprzewodową;

7.11 Serwer musi zapewniać funkcjonalności z zakresu zarządzania siecią:
7.11.1 hierarchizacji zarządzania siecią odzwierciedlająca hierarchię geograficzną tj. możliwość podziału sieci na kilka poziomów geograficznych np. region, kraj, miasto, budynek, piętro;
7.11.2 wizualizacji graficznej na mapie lokalizacji poszczególnych urządzeń sieciowych – automatyczne rozmieszczanie urządzeń na postawie adresów pocztowych;
7.11.3 możliwości wgrywania własnych planów budynków z dokładnością do poszczególnych pięter;
7.11.4 obsługi REST API;
7.11.5 integracji z system uwierzytelniania w celu otrzymywania informacji o tym jaki użytkownik jest związany z jakim urządzeniem, szczegółowej informacji o przebiegu procesu uwierzytelniania do sieci. Uwzględnienie tych danych w procesie wyznaczania indeksów jakości pracy użytkowników jak również w procesie diagnostyki problemów w sieci;
7.11.6 mechanizm automatycznej aktualizacji wersji systemu bezpośrednio z chmury producenta wtedy, kiedy pojawiają się nowe wersje;
7.11.7 wbudowane narzędzie do automatycznego tworzenia polityki QoS dla całej sieci w oparciu o wbudowane wzorce aplikacji, z możliwością tworzenia własnych wzorców. Możliwości dokonywania zmian w polityce i jej szybkiej implementacji oraz możliwość cofania zmian bez konieczności ręcznej rekonfiguracji urządzeń sieciowych;
7.11.8 automatycznego wykrywania urządzeń sieciowych w oparciu o SNMP, CLI, http, SSH;
7.11.9 możliwość tworzenia parametryzowanych wzorców konfiguracyjnych dla urządzeń w oparciu o język skryptowy;
7.11.10 inwentaryzacja urządzeń oraz oprogramowania;
7.11.11 zarządzania wersjami oprogramowania z możliwością wskazania wersji obowiązujących;
7.11.12 narzędzie do bezdotykowej konfiguracji urządzeń sieciowych (Plug and Play lub Zero Touch Deployment);
7.11.13 narzędzie do zdalnego uruchamiania aplikacji i zarządzania nimi na urządzeniach sieciowych wyposażonych w taką funkcjonalność;
7.11.14 możliwość definiowania profili sieciowych oraz parametrów sieciowych takich jak: serwery TACAS, Radius, NTP, Syslog, NetFlow, DNS, DHCP dla poszczególnych poziomów hierarchii sieciowej niezależnie lub dziedziczenie tych ustawień z poziomu wyższego w dół hierarchii. Centralne zarządzania parametrami dostępowymi do urządzeń wraz z możliwością ich zmiany dla jednego urządzenia, grupy urządzeń lub całej sieci;

7.12 Serwer musi zapewniać funkcjonalności z zakresu zarządzania siecią SDN (funkcje kontrolera SDN):
7.12.1 zarządzania i monitorowania sieci kampusoej SDN jako jednolitej sieci typu Network Fabric;
7.12.2 graficzny interfejs użytkownika umożliwiający tworzenie segmentacji i polityki bezpieczeństwa w sieci SDN jak również provisioning urządzeń sieciowych tworzących sieć typu Network Fabric;

7.12.3 funkcje centralnego kontrolera SDN umożliwiające centralne programowanie urządzeń oraz centralny monitoring i analizę strumieni telemetrycznych z sieci w celu wykrywania nieprawidłowości w jej działaniu;
7.12.4 centralnego zarządzania polityką bezpieczeństwa poprzez określenie relacji pomiędzy segmentami logicznymi w sieci SDN (grupami urządzeń, użytkowników lub aplikacji) z możliwością tworzenia kontraktów dla wymiany ruchu pomiędzy tymi grupami;
7.12.5 filtracji ruchu niezależnie od adresacji IP w oparciu o rolę użytkownika lub urządzenia w sieci i zdefiniowane relacje;
7.12.6 zarządzania pulami adresowymi używanymi w sieci SDN;
7.12.7 zarządzania sposobem uwierzytelniania w sieci Network Fabric na poziomie globalnym oraz na poziomie każdego z portów urządzeń dostępowych niezależnie;
7.12.8 logicznego podziału sieci na wiele sieci wirtualnych (VN);
7.12.9 logicznego podziału użytkowników i urządzeń na grupy i określenie relacji pomiędzy nimi;
7.12.10 tworzenia podsieci IP rozciągniętej na dowolne porty dostępowe w ramach Network Fabric;
7.12.11 umożliwiające filtrowanie ruchu pomiędzy urządzeniami pracującymi w jednej grupie logicznej i/lub podsieci IP jak również pomiędzy różnymi grupami logicznymi i/lub podsieciami IP bez konieczności stosowania ACL opartych o adresy IP;
7.12.12 automatyzacji procesu tworzenia Network Fabric (dodawania urządzeń, przypisywanie im roli w sieci, określania poziomów uwierzytelnienia użytkowników i urządzeń na brzegu sieci) bez konieczności używania linii komend (CLI));
7.12.13 automatycznego wykrywania urządzeń sieciowych;
7.12.14 narzędzia do automatycznego wykrywania nowo podłączonych urządzeń sieciowych i ich podłączenia do sieci podkładowej (underlay) wraz z konfiguracją urządzeń;
7.12.15 jednolitego i zunifikowanego rozwiązania dla sieci kampusowej przewodowej oraz bezprzewodowej tj. możliwość tworzenia Network Fabric obejmującej zarówno sieć przewodową jak i bezprzewodową.

7.13 Serwer musi zapewniać skalowalność:
7.13.1 systemu umożliwiając pracę w oparciu o pojedynczy appliance sieciowy (1 urządzenie – brak redundancji) lub w oparciu o klaster 3 appliance sieciowych (redundancja 2+1). W postępowaniu należy dostarczyć pojedyncze urządzenie;
7.13.2 system musi być dostarczony jako appliance sieciowy w wersji sprzętowej umożliwiającej uzyskanie następujących wartości skalowalności:
7.13.2.1 zarządzanie i monitorowanie 1000 urządzeń sieciowych (przełączniki / routery),
7.13.2.2 zarządzanie i monitorowanie 4000 radiowych punktów dostępowych WiFi,
7.13.2.3 monitorowanie 25 000 klientów sieci.

7.14 Wymagania dodatkowe dla serwera zarządzającego i monitorującego:
7.14.1 musi umożliwiać współpracę, z posiadanym przez Zamawiającego systemem Cisco Identity Services Engine (ISE) 2.4, przy budowaniu polityk bezpieczeństwa;
7.14.2 system musi współpracować z dostarczanymi przełącznikami i punktami dostępowymi - muszą one znajdować się na publikowanej przez producenta liście kompatybilności proponowanego rozwiązania. Jeżeli do ich obsługi potrzeba dodatkowych licencji, należy je dostarczyć w ilości takiej samej jak ilość dostarczanych przełączników i punktów dostępowych;
7.14.3 system musi współpracować z posiadanymi przez Zamawiającego urządzeniami– muszą one znajdować się na publikowanej przez producenta liście kompatybilności proponowanego rozwiązania. Zamawiający posiada następujące modele przełączników i punktów dostępowych, którymi chce zarządzać i które chce monitorować:
7.14.3.1 3 szt. przełączników Cisco Catalyst 3650 (WS-C3650-48TD-S)
7.14.3.2 12 szt. przełączników Cisco Catalyst 2960X w tym:
7.14.3.2.1 2 szt. WS-C2960X-48TD-L
7.14.3.2.2 3 szt. WS-C2960X-24TD-L
7.14.3.2.3 7 szt. WS-C2960X-24TS-L
7.14.3.3 81 szt. przełączników Cisco Catalyst 2960CX (WS-C2960CX-8TC-L)

7.14.3.4 20 szt. przełączników Cisco Catalyst 3560CX (WS-C3560CX-8TC-S)
7.14.3.5 3 szt. przełączników Cisco Catalyst 9300 (C9300-48T-E) z aktywną licencją DNA Essentials
7.14.3.6 2 szt. przełączników Cisco Catalyst 9500 (C9500-40X-A) z aktywną licencją DNA Premier
7.14.3.7 14 szt. przełączników Cisco Catalyst 9300 (C9300-48T-A) z aktywną licencją DNA Premier
7.14.3.8 7 szt. punktów dostępowych Cisco Aironet 2800 (AIR-AP2802I-E-K9)

7.15 Jeśli producent proponowanego rozwiązania do zarządzania i monitoringu wymaga, do obsługi posiadanych przez Zamawiającego urządzeń opisanych w punkcie 7.14.3., licencji/subskrypcji; to odpowiednie licencje/subskrypcje muszą zostać dostarczone wraz z serwerem. Wymagane jest dostarczenie najwyższych licencji (najwyższego poziomu licencji) przewidzianych dla danego modelu przełącznika zarówno przez producenta serwera do zarządzania i monitoringu jak i przez producenta posiadanych urządzeń sieciowych.
Np. w wypadku zaoferowania rozwiązania firmy Cisco wymagane jest dostarczenie subskrypcji DNA Advantage lub DNA Essentials w zależności od ich dostępności dla danego modelu urządzenia. Wyjątek stanowią posiadane przez Zamawiającego przełączniki, które posiadają już aktywne wymagane licencje w najwyższej wersji. Jeżeli licencje/subskrypcje są czasowe, wymagane jest dostarczenie ich na okres 36 miesięcy.

8 Wyposażenie dodatkowe – wymagania:

8.1 W ramach dostawy należy dostarczyć:

8.1.1 Jeden moduł interfejsów sieciowych Cisco C9300-NM-8X= do posiadanego przez Zamawiającego przełącznika Cisco Catalyst 9300 (C9300-48T-A).

8.1.2 Jeden zasilacz sieciowy Cisco PWR-C1-350WAC-P= do posiadanego przez Zamawiającego przełącznika Cisco Catalyst 9300 (C9300-48T-A).

8.1.3 Cztery moduły SFP+ 10G LRM. Moduły SFP+ muszą pochodzić od producenta dostarczanych przełączników celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzeń.

8.1.4 Cztery moduły SFP+ 10G SR. Moduły SFP+ muszą pochodzić od producenta dostarczanych przełączników celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzeń.

8.1.5 Cztery kable typu Direct Attach Cable (DAC) 10G SFP+ o długości 3m. Kable muszą pochodzić od producenta dostarczanych przełączników celem uniknięcia problemów z kompatybilnością i serwisowaniem urządzeń.

9 Wymagania serwisowe

9.1 Urządzenia muszą zostać objęte co najmniej 24-miesięcznym wsparciem serwisowym opartym na niezależnych od statusu partnerskiego Wykonawcy, usługach serwisowych producenta.

9.2 Okres wsparcia serwisowego będzie liczony od daty podpisania bez zastrzeżeń końcowego protokołu odbioru przedmiotu zamówienia.

9.3 Oferowane wsparcie serwisowe musi zapewnić Zamawiającemu przez cały okres trwania:

9.3.1 serwis świadczony w dni robocze w godzinach roboczych;

9.3.2 możliwość zgłoszenia awarii urządzenia bezpośrednio producentowi urządzenia (a nie tylko Wykonawcy zamówienia) wraz z możliwością otrzymania "z góry" urządzenia zamiennego wolnego od uszkodzeń, bez dodatkowych opłat, a jedynie pod warunkiem zwrotu wadliwego urządzenia;

9.3.3 bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail oraz WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją urządzeń;

9.3.4 możliwość pobierania bezpośrednio od producenta nowych wydań oprogramowania zgodnie z zapotrzebowaniem Zamawiającego, jednakże w ramach ogólnie dostępnej oferty producenta, a także w ramach wykupionego zestawu funkcjonalności oprogramowania i wykupionej konfiguracji urządzeń, wraz z wolnym od dodatkowych opłat prawem (tj. licencją) do korzystania z pobranego oprogramowania na zasadach określonych w warunkach licencyjnych dla użytkownika końcowego.

9.4 Naprawa lub wymiana urządzenia musi nastąpić nie później niż w następnym dniu roboczym od zgłoszenia.

9.5 Wraz z produktami ma zostać dostarczone oświadczenie producenta lub przedstawiciela producenta potwierdzające objęcie urządzeń pakietem serwisowym.

Załącznik nr 2 do SIWZ

FORMULARZ OFERTOWY

OFERTA

_____
ul. _____
00-000 _____

W postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych **na dostawę urządzeń sieciowych dla Sądu Najwyższego**.

A. DANE WYKONAWCY:

Osoba upoważniona do reprezentacji Wykonawcy/ów i podpisująca ofertę:……..

Wykonawca/Wykonawcy:……..

……

Adres:……..

……..

Osoba odpowiedzialna za kontakty z Zamawiającym:……

Dane teleadresowe, na które należy przekazywać korespondencję związaną z niniejszym postępowaniem:

faks……

e-mail……

Adres do korespondencji (jeżeli inny niż adres siedziby): ……..

……

B. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

5 przełączników sieciowych typ I

Producent ……

Model: …… Product number: ……

Okres gwarancji …….…… miesięcy

C. CENA OFERTOWA wyrażona w złotych netto i brutto

Za 5 przełączników sieciowych typ I

netto …….. zł (słownie zł: ……..)

brutto …….. zł (słownie zł: ……)

Za **1 z 5** przełączników sieciowych typ I

netto …….. zł (słownie zł: ……..)

brutto …….. zł (słownie zł: ……)

D. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

2 przełączniki sieciowe typ II

Producent ……

Model: …… Product number: ……

Okres gwarancji …….…… miesięcy
prowadzi do powstania u Zamawiającego obowiązku podatkowego: **TAK / NIE**

E. CENA OFERTOWA wyrażona w złotych netto i brutto

Za 2 przełączniki sieciowe typ II

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

Za **1 z 2** przełączników sieciowych typ II

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

F. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

Kontroler sieci bezprzewodowej

Producent ……

Model: …… Product number: ……

Okres gwarancji …….…… miesięcy

G. CENA OFERTOWA wyrażona w złotych netto i brutto

Za kontroler sieci bezprzewodowej

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

H. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

9 punktów dostępowych sieci bezprzewodowej

Producent ……

Model: …… Product number: ……

Okres gwarancji …….…… miesięcy

I. CENA OFERTOWA wyrażona w złotych netto i brutto

Za 9 punktów dostępowych sieci bezprzewodowej

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

Za **1 z 9** punktów dostępowych sieci bezprzewodowej

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

J. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

Serwer zarządzający i monitorujący

Producent ……

Model: …… Product number: ……

Okres gwarancji …….. miesięcy

K. CENA OFERTOWA wyrażona w złotych netto i brutto

Za serwer zarządzający i monitorujący

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

L. CENA OFERTOWA wyrażona w złotych netto i brutto

Za moduł interfejsów sieciowych Cisco C9300-NM-8X=

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

M. CENA OFERTOWA wyrażona w złotych netto i brutto

Za zasilacz sieciowy Cisco PWR-C1-350WAC-P=

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

N. CENA OFERTOWA wyrażona w złotych netto i brutto

Za 4 moduły SFP+ 10G LRM

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

Za **1 z 4** modułów SFP+ 10G LRM

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

O. CENA OFERTOWA wyrażona w złotych netto i brutto

Za 4 moduły SFP+ 10G SR

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

Za **1 z 4** modułów SFP+ 10G SR

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

P. CENA OFERTOWA wyrażona w złotych netto i brutto

Za 4 kable typu Direct Attach Cable (DAC) 10G SFP+ o długości 3m

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

Za **1 z 4** kabli typu Direct Attach Cable (DAC) 10G SFP+ o długości 3m

netto …….. zł (słownie zł: ……)

brutto …….. zł (słownie zł: ……)

Q. OŚWIADCZENIA:

1) zamówienie zostanie zrealizowane w terminie określonym w SIWZ oraz we wzorze umowy;
2) w cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia;
3) zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia oraz ze wzorem umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte;
4) uważamy się za związanych niniejszą ofertą przez okres **30 dni** licząc od dnia otwarcia ofert;
5) akceptujemy, iż zapłata za zrealizowanie zamówienia nastąpi na zasadach opisanych we wzorze umowy w terminie **do 21 dni** od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury;
6) wadium w wysokości **……. PLN** (słownie: **……**), zostało wniesione w dniu ....., w formie: ……;
7) prosimy o zwrot wadium (wniesionego w pieniądzu), na zasadach określonych w art. 46 ustawy PZP, na następujący rachunek: ……;

R. ZOBOWIĄZANIA W PRZYPADKU PRZYZNANIA ZAMÓWIENIA:

1) zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego;
2) zobowiązujemy się do dostarczenia przedmiotu zamówienia w terminie ….. dni licząc od daty podpisania umowy;
3) osobą upoważnioną do kontaktów z Zamawiającym w sprawach dotyczących realizacji umowy jest .....
e-mail: ……..……..…….tel./faks: .....

S. PODWYKONAWCY:

Podwykonawcom zamierzam powierzyć poniższe części zamówienia (jeżeli jest to wiadome, należy podać również dane proponowanych podwykonawców)

1) .....
2) .....
3) .....

T. Załączniki do formularza oferty:

Integralną część oferty stanowią następujące dokumenty:

1) .....
2) .....
3) .....
4) .....
5) .....
6) .....
7) .....
8) .....

Oferta została złożona na ..... kolejno ponumerowanych stronach.

Załącznik nr 3 do SIWZ

Umowa

na dostawę urządzeń sieciowych

zawarta w dniu ..... roku w Warszawie przez:

STRONY UMOWY

ZAMAWIAJĄCY

nazwa: Sąd Najwyższy

adres: *pl. Krasińskich 2/4/6*
00-951 Warszawa

który reprezentują:

... *Szef Kancelarii Pierwszego Prezesa Sądu Najwyższego*

... *Główny Księgowy Sądu Najwyższego, Dyrektor Biura Finansowego*

WYKONAWCA

nazwa: *...*

adres: *ul. ....., ...-... .....*

którą reprezentuje: ....

(NIP: ..., REGON: ..., wpis ujawniony w Centralnej Ewidencji i Informacji o Działalności Gospodarczej ze statusem „aktywny" z dnia zawarcia niniejszej umowy, działający we własnym imieniu i na własny rachunek)*

(NIP: ..., REGON: ..., wpis ujawniony w Rejestrze Przedsiębiorców w Krajowym Rejestrze Sądowym pod numerem KRS ...)*

W rezultacie dokonania wyboru Wykonawcy w trybie przetargu nieograniczonego – została zawarta umowa o poniższej treści.

§ 1

Przedmiot umowy

1. Przedmiotem niniejszej umowy jest wykonanie zamówienia polegającego na dostawie do Sądu Najwyższego fabrycznie nowych:
   1) ...*
2. Szczegółowa specyfikacja urządzeń zawarta jest w ofercie Wykonawcy, złożonej w dniu ...* br. w postępowaniu o zamówienie publiczne na dostawę urządzeń sieciowych, stanowiącej Załącznik nr 3 do umowy.

§ 2

Termin wykonania

Wykonawca zobowiązuje się do dostarczenia przedmiotu umowy w ciągu … dni od podpisania umowy.

§ 3

Warunki realizacji

1. Odbiór zamówienia nastąpi protokolarnie przez pracownika Biura Informatyki upoważnionego przez Dyrektora Biura Informatyki w Sądzie Najwyższym, po dostarczeniu przedmiotu umowy do siedziby Sądu Najwyższego: Warszawa, pl. Krasińskich 2/4/6.
2. W przypadku opóźnienia w dostarczeniu przedmiotu umowy ponad termin określony w § 2 Zamawiający naliczy kary umowne w wysokości 1% wartości umowy brutto za każdy dzień opóźnienia, nie więcej jednak niż 10% wartości umowy brutto, z wyjątkiem sytuacji, gdy opóźnienie jest następstwem okoliczności, za które winę ponosi Zamawiający.
3. Gdy opóźnienie w dostarczeniu przedmiotu umowy przekroczy 10 dni od terminu określonego w § 2, Zamawiający może odstąpić od umowy po 3 dniach od powiadomienia Wykonawcy o tym zamiarze. W takim przypadku niezależnie od kar określonych w ust. 2 Wykonawca zapłaci Zamawiającemu dodatkową karę umowną w wysokości 5% wartości umowy brutto, z wyjątkiem sytuacji, gdy niewykonanie umowy jest następstwem okoliczności, za które winę ponosi Zamawiający.
4. Należność z tytułu kar umownych Zamawiający potrąci z należności przysługującej Wykonawcy, na co Wykonawca wyraża zgodę.

§ 4

Warunki gwarancji i Serwisu

1. Wykonawca (w imieniu producenta) udziela wsparcia na przedmiot umowy, co do jego jakości i funkcjonalności, na okres …*
2. Okres wsparcia rozpocznie się w dniu, w którym przedmiot umowy zostanie protokolarnie odebrany.
3. Obsługą serwisowo – gwarancyjną w ramach zapewnionego wsparcia producenckiego będzie zajmować się Wykonawca. Wykonawca zapewnia następujący tryb obsługi serwisowo – gwarancyjnej:
   1) przyjęcie zgłoszenia o awarii od poniedziałku do piątku w godz. 8 – 16,
   2) zgłoszenia będą kierowane telefonicznie na nr … oraz niezwłocznie potwierdzane faksem na nr … lub pocztą elektroniczną na adres …, na formularzu określonym w Załączniku nr 2 do umowy; osoby upoważnione ze strony Zamawiającego wymienione są w Załączniku nr 1 do umowy,
   3) naprawa urządzeń:
      a) nastąpi w dniu roboczym następującym po dniu zgłoszenia,

b) zostanie wykonana przez producenta sprzętu sieciowego lub przez autoryzowanego partnera serwisowego producenta sprzętu sieciowego,

c) nastąpi w siedzibie Zamawiającego, chyba że niezbędna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanego partnera serwisowego, wówczas koszt transportu do i z naprawy pokrywa Wykonawca,

4) jeśli naprawa nie będzie możliwa w wymaganym terminie (pkt 3 lit. a), to w następnym dniu roboczym dostarczony zostanie sprzęt zastępczy o identycznych lub lepszych parametrach, do użytkowania przez Zamawiającego do czasu usunięcia awarii,

5) za każdy dzień opóźnienia usunięcia awarii sprzętu wymienionego w § 1 ust. 1 Zamawiający obciąży Wykonawcę karą umowną w wysokości 1000 zł,

6) naliczenie kar umownych nie zwalnia Wykonawcy ze zobowiązań wynikających z umowy,

7) kara umowna będzie płatna w terminie 14 dni od dnia doręczenia przez Zamawiającego żądania zapłaty.

4. Zamawiający zobowiązuje się do udzielania Wykonawcy pomocy niezbędnej do sprawnego wywiązywania się z umowy, w tym w szczególności umożliwienia dostępu do pomieszczeń i urządzeń.

5. Zamawiający zastrzega sobie prawo do odszkodowania uzupełniającego przewyższającego wysokość kar umownych na zasadach ogólnych wynikających z Kodeksu cywilnego.

§ 5

Cena i warunki płatności

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy łącznie kwotę brutto … zł (słownie zł: … i …/100). Na kwotę zapłaty dla Wykonawcy złożą się: wartość przedmiotu umowy netto … zł (słownie zł: …) oraz podatek VAT (23%) od przedmiotu zamówienia opisanego w § 1 ust. 1 w wysokości … zł (słownie zł: … i …/100). *

2. Strony ustalają, iż zapłata Wykonawcy będzie dokonana przez Zamawiającego po protokolarnym odbiorze przedmiotu zamówienia, w ciągu 21 dni od daty otrzymania prawidłowo wystawionej faktury przez Zamawiającego.

3. Płatność dla Wykonawcy będzie dokonana przelewem przez Zamawiającego na konto Wykonawcy wskazane na fakturze.

4. Za datę dokonania płatności dla Wykonawcy uznaje się datę złożenia polecenia przelewu przez Zamawiającego.

5. Za opóźnienie w zapłacie Zamawiający zapłaci Wykonawcy za każdy dzień opóźnienia odsetki ustawowe za opóźnienie w transakcjach handlowych.

§ 6

Zmiany Umowy

1. Zamawiający zastrzega sobie prawo do zmian treści umowy stosownie do przepisów prawa powszechnie obowiązującego oraz działań organów administracji.

2. Wszelkie zmiany w Umowie będą mogły być dokonywane wyłącznie w zakresie dopuszczonym ustawą Prawo Zamówień Publicznych, wymagają zgodnej woli Stron oraz zachowania formy pisemnej, pod rygorem nieważności.
3. Strony przewidują możliwość wprowadzenia istotnych zmian umowy w stosunku do treści oferty w przypadku, gdy:
    1) nastąpi zmiana nazwy handlowej lub innego oznaczenia towaru wskazanego w ofercie nie powodująca zmiany przedmiotu umowy;
    2) zmiany terminu realizacji dostaw z uwagi na:
        a) konieczność zmiany sposobu wykonania umowy, o ile zmiana taka jest konieczna w celu prawidłowego wykonania umowy,
        b) okoliczności wynikających z działania siły wyższej, uniemożliwiających wykonanie przedmiotu umowy;
    3) nastąpi zmiana lub rezygnacja z Podwykonawcy, przy pomocy którego Wykonawca realizuje przedmiot umowy, po uprzedniej akceptacji Zamawiającego;
    4) nastąpi zmiana przepisów prawa powszechnie obowiązującego, która ma wpływ na termin, sposób lub zakres realizacji przedmiotu umowy;
    5) nastąpi konieczność dostarczenia innego Sprzętu, posiadającego parametry nie gorsze niż zaoferowane przez Wykonawcę w ofercie złożonej w postępowaniu, spowodowana zakończeniem produkcji Sprzętu lub wycofaniem danego modelu z produkcji lub obrotu na terytorium Rzeczypospolitej Polskiej;
    6) nastąpi zmiana stron w umowie wynikających ze zmian organizacyjnych niezależnych od Zamawiającego, np. przez podział Jednostki lub połączenie Jednostek;
    7) nastąpi zmiana wynikająca z omyłki pisarskiej.
4. Warunkiem dokonania zmian, o których mowa w ust. 3, jest złożenie pisemnego wniosku przez stronę inicjującą zmianę, zawierającego m.in. dokładny opis propozycji zmian oraz uzasadnienie celowości tych zmian lub oświadczenie producenta Sprzętu - w przypadku, o którym mowa w ust. 3 pkt 5. Zmiany obowiązują z dniem podpisania aneksu lub ich akceptacji przez drugą stronę.
5. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Zamawiający może wyrazić zgodę lub odmówić jej udzielenia - bez podawania uzasadnienia odmowy.
6. Dodatkowo Strony przewidują możliwość wprowadzenia istotnych zmian umowy w przypadku zmiany:
    1) stawki podatku od towarów i usług;
    2) nazwy, adresu lub statusu Wykonawcy.
7. Warunkiem dokonania zmian, o których mowa w ust. 6, jest złożenie pisemnego wniosku przez stronę inicjującą zmianę, zawierającego m.in. dokładny opis propozycji zmian oraz uzasadnienie, że zmiany, o których mowa powyżej, będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę.
8. Zamawiający jest uprawniony do żądania od Wykonawcy wyjaśnień i dowodów na okoliczności zawarte przez niego we wniosku o zmianę wynagrodzenia w celu jednoznacznego rozstrzygnięcia, czy zmiana wynagrodzenia jest zasadna.

9. Zmiana wynagrodzenia może nastąpić nie wcześniej niż z dniem wejścia w życie aktu normatywnego wprowadzającego zmianę, która stanowi podstawę do wystąpienia z wnioskiem o zmianę wynagrodzenia.

§ 7

Postanowienia końcowe

1. Zmiana niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.
2. Niedopuszczalne są takie zmiany postanowień zawartej umowy oraz wprowadzenie do niej nowych postanowień, niekorzystnych dla Zamawiającego, jeżeli przy ich uwzględnieniu należałoby zmienić treść oferty, na podstawie której dokonano wyboru oferenta.
3. W przypadku, gdy w trakcie realizacji Umowy będą przetwarzane dane osobowe, Wykonawca zobowiązany jest do stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 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 (dalej „RODO"), przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz i innych przepisów prawa w tym zakresie.
4. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy Kodeksu Cywilnego i ustawy Prawo Zamówień Publicznych.
5. Spory wynikłe na tle realizacji niniejszej umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
6. Umowę niniejszą sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
7. Załączniki do umowy:
   1) Osoby uprawnione do reprezentowania Zamawiającego w procedurach związanych z obsługą gwarancyjną (Załącznik nr 1),
   2) Formularz zgłoszenia serwisowego (Załącznik nr 2),
   3) Oferta Wykonawcy złożona w dniu … *. (Załącznik nr 3),

   stanowią jej integralną część.

ZAMAWIAJĄCY WYKONAWCA

*- treść umowy zostanie dostosowana do oferty wybranego Wykonawcy

Załącznik nr 1 do umowy na dostawę urządzeń sieciowych

Osoby uprawnione do reprezentowania Zamawiającego w procedurach związanych z obsługą gwarancyjną:

Maciej Pajączkowski

Piotr Góralski

Jarosław Boguski

Załącznik nr 2 do umowy na dostawę urządzeń sieciowych

Zgłoszenie serwisowe

Data zgłoszenia:	
Godz. zgłoszenia:	

Do:	Zgłaszający:
Tel: (__) _____ Fax: (__) _____ e-mail: _____@_____	Sąd Najwyższy pl. Krasińskich 2/4/6 00-951 Warszawa Tel: (22) 358 84 09 Fax. (22) 358 90 30

Nazwa sprzętu:	Numer seryjny:

Opis usterki:

Naprawa gwarancyjna

Osoba zgłaszająca usterkę:	
Podpis:	

Załącznik nr 4 do SIWZ

Sąd Najwyższy
pl. Krasińskich 2/4/6
00-951 Warszawa

Wykonawca:
.....
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG) reprezentowany przez:

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

Oświadczenie wykonawcy w zakresie braku PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA lub w zakresie braku postępowania naprawczego

Na potrzeby postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest dostawa urządzeń sieciowych dla Sądu Najwyższego, oświadczam, że:

1) nie wydano/wydano* wobec mnie/nas* prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne

   W przypadku takiego wyroku lub decyzji należy załączyć dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności

2) nie orzeczono/orzeczono* wobec mnie/nas* tytułem środka zapobiegawczego zakazu ubiegania się o zamówienie publiczne;

.....
(podpis**, miejscowość, data)
UWAGA: NINIEJSZE OŚWIADCZENIE SKŁADA ODRĘBNIE KAŻDY Z WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O ZAMÓWIENIE ORAZ INNY PODMIOT NA KTÓREGO ZDOLNOŚCIACH LUB SYTUACJI POLEGA WYKONAWCA.
W przypadku, gdy którekolwiek ze zdarzeń opisanych w pkt 1-2 zaistniało, poniżej należy opisać postępowanie naprawcze.