Urząd Transportu Kolejowego Warszawa dn. lutego 2014r.

ul. Chałubińskiego 4

00‐928 Warszawa

**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**

**na zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem, zakup i dostarczenie przełączników warstwy drugiej wraz z osprzętem i wsparciem przy wdrożeniu
oraz zakup i dostarczenie dysków do macierzy**

Znak postępowania: BAF-2311-92/2014

|  |  |  |
| --- | --- | --- |
| Za komisję przetargową: | Za zgodność z przepisami prawnymi: | Zatwierdził: |
|  |  |  |
| Wacław CzarnotaPrzewodniczący Komisji PrzetargowejDyrektor Biura Administracyjno-FinansowegoUrzędu Transportu Kolejowegoz siedzibą w Warszawie | Marcin TrelaRadca prawnyUrzędu Transportu Kolejowegoz siedzibą w Warszawie | Radosław PacewiczZastępujący Dyrektora GeneralnegoUrzędu Transportu Kolejowegoz siedzibą w Warszawie |

1. **NAZWA** **I** **ADRES** **ZAMAWIAJĄCEGO**
	1. Nazwa: Urząd Transportu Kolejowego
	2. Adres: 00‐928 Warszawa, ul. Chałubińskiego 4
	3. Dane teleadresowe i internetowe:
		1. tel.: (0‐22) 630‐18‐80, faks: (0‐22) 630‐18‐91,
		2. e‐mail: zamowieniapubliczne@utk.gov.pl, strona: [www.utk.gov.pl](http://www.utk.gov.pl/)
2. **TRYB** **UDZIELENIA** **ZAMÓWIENIA**
	1. Postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2013r., poz. 907 z późn. zm.), zwanej dalej „Ustawą PZP”.
	2. Wartość zamówienia nie przekracza wyrażonej w złotych polskich równowartości kwoty 134.000 euro.
3. **OPIS** **PRZEDMIOTU** **ZAMÓWIENIA**
	1. Przedmiotem zamówienia jest **zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem, zakup i dostarczenie przełączników warstwy drugiej wraz z osprzętem i wsparciem przy wdrożeniu oraz zakup i dostarczenie dysków do macierzy**.
	2. Szczegółowy opis przedmiotu zamówienia, przewidywaną ilość zamawianego asortymentu, minimalne wymagania, funkcjonalności oraz parametry, jakie spełniać muszą w/w. wraz z informacjami, oraz innego rodzaju obowiązków nakładanych na Wykonawcę ‐ zawiera Opis Przedmiotu Zamówienia, zwany dalej OPZ, stanowiący Załącznik nr 1 do SIWZ.
	3. Opis zasad oraz warunków szczegółowych realizacji umowy, zawiera wzór umowy, będący Załącznikiem nr 2 do SIWZ
	4. Kody Wspólnego Słownika Zamówień (CPV): 32500000-8 Urządzenia i artykuły telekomunikacyjne, 80500000-9 -Usługi szkoleniowe, 30233141-1 Nadmiarowa macierz niezależnych dysków (RAID).
	5. Zamawiający dopuszcza składanie ofert częściowych:
		1. Zadanie 1 – Zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem oraz zakupem i dostarczeniem sprzętu i osprzętu sieciowego IT wraz z wsparciem przy wdrożeniu.
		2. Zadanie 2 – Zakup i dostarczenie dysków do macierzy dyskowej.
4. **TERMIN** **WYKONANIA** **ZAMÓWIENIA**
	1. Zamawiający ma zamiar zawrzeć umowę obowiązującą od dnia jej zawarcia.
	2. Termin wykonania zamówienia w zakresie:
		1. Zadanie 1 – Zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem oraz zakupem i dostarczeniem sprzętu i osprzętu sieciowego IT wraz z wsparciem przy wdrożeniu: w zakresie dostawy 30 dni od podpisania umowy, w zakresie szkolenia 6 miesięcy od podpisania umowy ;
		2. Zadanie 2 – Zakup i dostarczenie dysków do macierzy dyskowej: 14 dni od podpisania umowy;
5. **WARUNKI** **UDZIAŁU** **W** **POSTĘPOWANIU** **ORAZ** **OPIS** **SPOSOBU** **DOKONYWANIA** **OCENY** **SPEŁNIANIA** **WARUNKÓW** **UDZIAŁU** **W POSTĘPOWANIU**
	1. O udzielenie zamówienia mogą się ubiegać Wykonawcy:
		1. co do których nie ma podstaw do wykluczenia z postępowania wskazanych w art. 24 ust. 1 oraz art. 24 ust. 2 Ustawy PZP oraz spełniający jednocześnie następujące warunki:
			1. posiadają uprawnienie do wykonywania określonej działalności i czynności będących przedmiotem niniejszego zamówienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień,
			2. posiadają niezbędną wiedzę i doświadczenie, oraz dysponują odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania zamówienia, tj.:
				1. Wykonawca musi być autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam jest producentem przedmiotu zamówienia.
				2. Wykonawca musi zatrudniać minimum 2 certyfikowanych przez producenta inżynierów wsparcia technicznego przeszkolonych w zakresie przedmiotowego sprzętu i oprogramowania
			3. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
	2. Wykonawca może polegać na potencjale technicznym lub osobach zdolnych do wykonania zamówienia innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.
	3. Ocena spełniania warunków odbędzie się zgodnie z formułą „spełnia / nie spełnia”, na podstawie złożonych wraz z ofertą dokumentów oraz oświadczeń.
	4. O udzielenie zamówienia mogą ubiegać się Wykonawcy występujący wspólnie (m.in. konsorcjum, spółka cywilna).
	5. Wykonawcy samodzielnie składający ofertę oraz każdy z Wykonawców składających wspólną ofertę (m.in. konsorcjum, spółka cywilna), musi spełnić warunek niewykluczenia z postępowania, zgodnie z pkt 5.1. SIWZ.
	6. Złożenie przez Wykonawcę nieprawdziwych informacji, mających wpływ na wynik prowadzonego postępowania, spowoduje wykluczenie Wykonawcy z postępowania, na podstawie art. 24 ust. 2 pkt 3 Ustawy PZP.
6. **WYKAZ** **OŚWIADCZEŃ I** **DOKUMENTÓW** **WYMAGANYCH** **W** **CELU** **POTWIERDZENIA** **SPEŁNIANIA** **WARUNKÓW** **UDZIAŁU** **W POSTĘPOWANIU**
	1. W celu potwierdzenia spełniania warunków udziału w postępowaniu, oraz w celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia – Wykonawca musi złożyć następujące dokumenty:
		1. Oświadczenie Wykonawcy (część Formularza Ofertowego, będącego załącznikiem nr 3 do SIWZ):
			1. o spełnieniu warunków udziału w postępowaniu o zamówienie publiczne oraz
			2. o braku podstaw do wykluczenia z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 Ustawy PZP (tj. o niefigurowaniu w Kartotece Podmiotów Zbiorowych Krajowego Rejestru Karnego, oraz o niefigurowaniu w Kartotece Karnej Krajowego Rejestru Karnego ‐ w zakresie określonym w art. 24 ust. 1 pkt 1‐11 Ustawy PZP) oraz w art. 24 ust. 2 Ustawy PZP, oraz
			3. o niezaleganiu z opłacaniem podatków (Urząd Skarbowy), lub uzyskaniu przewidzianego prawem zwolnienia, odroczenia lub rozłożeniu na raty zaległych płatności lub wstrzymaniu w całości wykonania decyzji właściwego organu, oraz
			4. o niezaleganiu z opłacaniem składek na ubezpieczenia zdrowotne i społeczne (Zakład Ubezpieczeń Społecznych lub Kasa Rolniczego Ubezpieczenia Społecznego), lub uzyskaniu przewidzianego prawem zwolnienia, odroczenia lub rozłożenia na raty zaległych płatności lub wstrzymaniu w całości wykonania decyzji właściwego organu
		2. Aktualny odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji (dla osób wykonujących jednoosobowo działalność gospodarczą – wypis z centralnej ewidencji i informacji o działalności gospodarczej; dla spółki cywilnej – wypis z centralnej ewidencji i informacji o działalności gospodarczej wszystkich wspólników, dla pozostałych – wypis z KRS), wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, (dokumenty w formie oryginału lub kopii poświadczonych za zgodność z oryginałem przez Wykonawcę lub osobę upoważnioną, z zachowaniem sposobu reprezentacji);
		3. Dokument potwierdzający, iż Wykonawca jest: autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam jest producentem przedmiotu zamówienia, oraz oświadczenie, iż Wykonawca zatrudnia minimum 2 certyfikowanych przez producenta inżynierów wsparcia technicznego przeszkolonych w zakresie przedmiotowego sprzętu i oprogramowania.
		4. Ilustrowane foldery producenta, rysunki, opisy techniczne, potwierdzające, że oferowany przedmiot zamówienia spełnia minimalne parametry określone przez Zamawiającego w Opisie Przedmiotu Zamówienia w zał. nr 1 do SIWZ.
		5. Oświadczenie Wykonawcy (część Formularza Ofertowego, będącego załącznikiem nr 3 do SIWZ) o tym, iż Wykonawca należy/nie należy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 Ustawy PZP.
		6. Oświadczenie Wykonawcy, że:
			1. oferowany przedmiot zamówienia spełnia warunki określone w Opisie Przedmiotu Zamówienia z załącznika nr 1 do SIWZ, w tym, w szczególności – dostarczony przedmiot zamówienia jest fabrycznie nowy, pochodzi z oficjalnego kanału sprzedaży producenta na rynek polski, oraz objęty jest gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne
			2. oferowany przedmiot zamówienia spełnia warunki zgodności wynikające z wszelkich, powszechnie obowiązujących, określonych przepisami prawa norm na terenie Rzeczpospolitej Polskiej, w tym zakresie;
	2. W przypadku oferty składanej przez Wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego (konsorcjum, spółka cywilna), oświadczenia oraz dokumenty ‐ składa każdy z Wykonawców oddzielnie.
	3. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium RP – stosuje się odpowiednio zapisy §4 Rozporządzenia Prezesa Rady Ministrów z dn. 19.02.2013 r w sprawie rodzajów dokumentów, jakie może żądać zamawiający od wykonawcy, oraz form, w jakich te dokumenty mogą być składane (DZ.U.2013 poz.231);
7. **SPOSÓB** **POROZUMIEWANIA** **SIĘ ZAMAWIAJĄCEGO** **Z** **WYKONAWCAMI** **ORAZ** **PRZEKAZYWANIA** **OŚWIADCZEŃ LUB DOKUMENTÓW,** **A** **TAKŻE** **WSKAZANIE** **OSÓB** **UPRAWNIONYCH** **DO** **POROZUMIEWANIA** **SIĘ Z** **WYKONAWCAMI**
	1. W postępowaniu o udzielenie zamówienia oświadczenia, wnioski, zawiadomienia oraz informacje zamawiający i wykonawcy przekazują faksem, pisemnie lub drogą elektroniczną.
	2. Każda ze stron na żądanie drugiej potwierdza fakt otrzymania oświadczenia, wniosku, zawiadomienia lub informacji, otrzymanej w formie faksowej lub elektronicznej.
		1. Osobami uprawnionymi do kontaktu z Wykonawcami jest:
			1. W sprawach merytorycznych: Krzysztof Rumniak, mail: krzysztof.rumniak@utk.gov.pl
			2. W sprawach formalno-prawnych: Joanna Kochańska, mail: joanna.kochanska@utk.gov.pl
8. **WYMAGANIA** **DOTYCZĄCE** **WADIUM**
	1. Zamawiający nie wymaga wniesienia wadium.
9. **TERMIN** **ZWIĄZANIA** **OFERTĄ**
	1. Termin związania ofertą złożoną w przedmiotowym postępowaniu wynosi 30 dni.
10. **OPIS** **SPOSOBU** **PRZYGOTOWYWANIA** **OFERTY**
	1. Na ofertę składają się:
		1. Wypełniony Formularz Oferty wraz z Formularzem Cenowym oraz wymaganymi oświadczeniami ‐ załącznik nr 3 do SIWZ;
		2. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
		3. Dokument potwierdzający, iż Wykonawca jest: autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam jest producentem przedmiotu zamówienia, oraz oświadczenie, iż Wykonawca zatrudnia minimum 2 certyfikowanych przez producenta inżynierów wsparcia technicznego prze-szkolonych w zakresie przedmiotowego sprzętu i oprogramowania.
		4. Ilustrowane foldery producenta, rysunki, opisy techniczne, potwierdzające, że oferowany przedmiot zamówienia spełnia minimalne parametry określone przez Zamawiającego w Opisie Przedmiotu Zamówienia w załącznik nr 1 do SIWZ.
		5. Oświadczenie Wykonawcy, że:
			1. oferowany przedmiot zamówienia spełnia warunki określone w Opisie Przedmiotu Zamówienia z załącznika nr 1 do SIWZ, w tym, w szczególności – dostarczony przedmiot zamówienia jest fabrycznie nowy, pochodzi z oficjalnego kanału sprzedaży producenta na rynek polski, oraz objęty jest gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne
			2. oferowany przedmiot zamówienia spełnia warunki zgodności wynikające z wszelkich, powszechnie obowiązujących, określonych przepisami prawa norm na terenie Rzeczpospolitej Polskiej, w tym zakresie;
	2. Wykonawca powołujący się przy wykazywaniu spełniania Warunków udziału w postępowaniu na potencjał innych podmiotów, które będą brały udział w realizacji części zamówienia, przedkłada także dokumenty dotyczące tego podmiotu w zakresie wymaganym dla Wykonawcy, określonym w pkt. 6 SIWZ
	3. W przypadku złożenia oferty przez podmioty występujące wspólnie (np. konsorcjum, spółka cywilna) – konieczne jest załączenie do oferty upoważnienie do podpisania oferty (o ile upoważnienie to nie wynika z innych dokumentów dołączonych do oferty) dla wspólnego pełnomocnika. Dokument pełnomocnictwa musi być złożony w postaci oryginału (lub notarialnie poświadczonej kopii);
	4. Oferta powinna być sporządzona: w formie pisemnej, w języku polskim, na kolejno ponumerowanych i podpisanych kartkach oraz podpisana na końcu oferty (przez osobę upoważnioną do reprezentacji Wykonawcy), a numeracja kartek powinna rozpoczynać się od numeru 1, umieszczonego na pierwszej kartce oferty,
	5. Podpisy złożone przez Wykonawcę powinny umożliwiać ocenę tego, czy oferta została złożona przez osoby upoważnione do reprezentacji Wykonawcy.
	6. Dokumenty są składane w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez Wykonawcy. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu wyłącznie wtedy, gdy złożona przez Wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jej prawdziwości.
	7. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
	8. Oferta (w tym wszelkie oświadczenia i zaświadczenia dołączone do niej) jest jawna, z wyjątkiem informacji stanowiących tajemnice przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, a Wykonawca składając ofertę zastrzegł w odniesieniu do tych informacji, że nie mogą one być udostępnione innym uczestnikom postępowania.
	9. Jeden Wykonawca może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub złożenie ofert wariantowych /alternatywnych spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
	10. Wykonawca winien zamieścić ofertę wraz ze wszystkimi załącznikami w zapieczętowanej kopercie opatrzonej: danymi wykonawcy (nazwa i adres lub pieczęć firmowa Wykonawcy), oraz oznaczona jako: „*Oferta – na zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem, zakup i dostarczenie przełączników warstwy drugiej wraz z osprzętem i wsparciem przy wdrożeniu oraz zakup i dostarczenie dysków do macierzy (BAF-2311-92/2014)‐ Nie otwierać przed 10.02.2014r przed godz. 10.30*”
11. **MIEJSCE** **ORAZ** **TERMIN** **SKŁADANIA** **I** **OTWARCIA** **OFERT**
	1. Ofertę należy złożyć w terminie do 10.02.2014r do godziny 10.00 do sekretariatu Biura Administracyjno – Finansowego UTK (pok. 401a) ‐ Urząd Transportu Kolejowego, ul. Chałubińskiego 4, 00‐928 Warszawa.
	2. Oferty można przesłać pocztą (decyduje data wpływu do Zamawiającego) lub składać bezpośrednio w siedzibie Zamawiającego.
	3. Otwarcie ofert nastąpi w siedzibie Zamawiającego: Urząd Transportu Kolejowego, ul. Chałubińskiego 4, 00‐928 Warszawa, w sali nr 420 (IV piętro) w dniu 10.02.2014r o godzinie 10.30.
	4. Otwarcie ofert jest jawne.
	5. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
	6. Podczas otwarcia ofert Zamawiający poda nazwy (firmy) oraz adresy (siedziby) Wykonawców, a także informacje dotyczące cen zawartych w ofertach, terminu wykonania zamówienia, warunków płatności i okresu gwarancji.
12. **OPIS** **SPOSOBU** **OBLICZENIA** **CENY**
	1. Wykonawca zobowiązany jest do wypełnienia Formularza Ofertowego, stanowiącego załącznik nr 3 do niniejszej SIWZ i określenia w nim cen jednostkowych dla każdego elementu składowego przedmiotu zamówienia, oraz sum zbiorczych, w zakresie każdej z części (zadania) postepowania, na jakie składa ofertę.
	2. Jako cenę oferty w zakresie danej części (zadania) postępowania, rozumie się cenę brutto tejże części, obliczoną w następujący sposób:
		1. Wykonawca – w zakresie danej części (zadania) - przemnoży ilość zamawianych elementów składowych przedmiotu zamówienia przez cenę jednostkową netto za dany element składowy, uzyskując w ten sposób wartość netto danego elementu składowego przedmiotu zamówienia.
		2. Wykonawca – w zakresie danej części (zadania) - do uzyskanej wartości netto zamawianych artykułów doliczy podatek VAT w obowiązującej wysokości, uzyskując w ten sposób wartość brutto danego elementu składowego przedmiotu zamówienia.,
		3. Wykonawca – w zakresie danej części (zadania) - zsumuje wartości brutto z każdej pozycji Formularza Ofertowego (wszystkim elementów składowych przedmiotu zamówienia), uzyskując w ten sposób łączną cenę brutto oferty.
13. **KRYTERIA** **OCENY** **OFERT** **I** **ICH** **ZNACZENIE** **ORAZ** **SPOSÓB** **OCENY** **OFERT**
	1. Kryterium oceny oferty w zakresie każdej z części (zadań) w niniejszym postępowaniu jest cena brutto (waga: 100%).
	2. W kryterium oceny ofert zostanie zastosowany wzór: „Ocena punktowa = (najniższa łączna cena brutto oferty / cena brutto oferty badanej) x 100 pkt
	3. Za najkorzystniejszą zostanie uznana oferta, spośród ofert spełniających warunki określone w SIWZ, która uzyska najwyższą liczbę punktów.
	4. Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający jednocześnie zawiadomi Wykonawców, którzy złożyli oferty (podając uzasadnienie faktyczne i prawne):
		1. o Wykonawcach, którzy zostali wykluczeni z postępowania oraz
		2. o Wykonawcach, których oferty zostały odrzucone, oraz
		3. o wyborze najkorzystniejszej oferty,
	5. Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający umieści również informacje o wyborze najkorzystniejszej oferty na własnej stronie internetowej i w swojej siedzibie w miejscu publicznie dostępnym (tablica ogłoszeń na IV piętrze w siedzibie Zamawiającego)
14. **FORMALNOŚCI** **PO** **WYBORZE** **OFERTY** **W** **CELU** **ZAWARCIA** **UMOWY**
	1. Zamawiający, po skutecznym wyborze ofert najkorzystniejszych, poinformuje wybranego Wykonawcę w zakresie każdej z części, o miejscu, terminie i sposobach zawarcia umowy.
15. **WYMAGANIA** **DOTYCZĄCE** **ZABEZPIECZENIA** **NALEŻYTEGO** **WYKONANIA** **UMOWY**
	1. Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.
16. **WZÓR** **UMOWY**
	1. Opis zasad oraz warunków szczegółowych realizacji umowy, zawiera wzór umowy, będący Załącznikiem nr 2 do SIWZ
17. **POUCZENIE** **O** **ŚRODKACH** **PRAWNYCH** **PRZYSŁUGUJĄCYCH** **WYKONAWCY** **W** **TOKU** **POSTĘPOWANIA**
	1. Wykonawcom przysługują środki ochrony prawnej określone w Dziale VI ustawy PZP (art. 179 ‐198g ustawy PZP),
18. **INNE** **INFORMACJE**
	1. Zamawiający nie dopuszcza złożenia ofert wariantowych.
	2. Zamawiający przewiduje możliwość udzielania zamówień uzupełniających w oparciu o art. 67 ust. 1 pkt 7 Ustawy PZP – do 20% wartości zamówienia.
	3. Zamawiający nie przewiduje zamiaru zawarcia umowy ramowej.
	4. Zamawiający nie przewiduje ustanowienia dynamicznego systemu zakupów.
	5. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.
	6. Zamawiający nie wymaga, aby całość przedmiotu zamówienia została zrealizowana wyłącznie przez Wykonawcę, tzn. Wykonawca może powierzyć realizację całości/części zamówienia podwykonawcom. W takim wypadku Zamawiający wymaga do Wykonawcy informacji w Formularzu Ofertowym, jaka część zamówienia zostanie powierzona podwykonawcom.
19. **ZAŁĄCZNIKI** **DO** **SIWZ**
	1. Opis Przedmiotu Zamówienia
	2. Wzór umowy
	3. Formularz Ofertowy

**Załącznik** **nr** **1**

**Opis przedmiotu zamówienia**

w postępowaniu na zakup i dostarczenie wielozadaniowego systemu zabezpieczeń

sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem, zakup i dostarczenie

przełączników warstwy drugiej wraz z osprzętem i wsparciem przy wdrożeniu
oraz zakup i dostarczenie dysków do macierzy

**Część 1 (zadanie nr 1).**

**ZAKUP I DOSTARCZENIE WIELOZADANIOWEGO SYSTEMU ZABEZPIECZEŃ SIECIOWYCH WRAZ Z WSPARCIEM PRZY WDROŻENIU I SZKOLENIEM, ORAZ ZAKUP I DOSTARCZENIE DYSKÓW DO MACIERZY DYSKOWEJ WRAZ Z WSPARCIEM PRZY WDROŻENIU.**

1. Przedmiotem Zamówienia jest:
2. Zakup i dostarczenie - **wielozadaniowego systemu zabezpieczeń sieciowych** wraz ze:
	1. wsparciem przy wdrożeniu w wymiarze 50h przez inżyniera certyfikowanego przez producenta systemu, oraz
	2. autoryzowanym przez producenta systemu szkoleniem z użytkowania sytemu - na terenie Warszawy dla jednego administratora zamawiającego w wymiarze min 35 godzin. Termin szkolenia w ciągu 6 miesięcy od dnia podpisania umowy - ustalony z Zamawiającym.
3. Zakup i dostarczenie **sprzętu i osprzętu sieciowego IT**, na które składać się będzie:
	1. Zakup i dostarczenie **przełączników sieci typu LAN PoE warstwy 2 o stałej konfiguracji z możliwością pracy w stosie** – ilość: 3 (trzy) sztuki,
	2. Zakup i dostarczenie **wkładki typu SFP+ kompatybilne z dostarczanymi** w pkt I.2a) (w zadaniu nr 1) **przełącznikami sieci LAN** PoE warstwy 2 o stałej konfiguracji z możliwością pracy w stosie – ilość: 6 (sześć) sztuk
	3. Zakup i dostarczenie **patchcordu światłowodowego typu LC‐LC, 50/125um**, o długości 2 m – ilość: 6 szt.
	4. **Wsparcie przy wdrożeniu urządzeń** określonych w pkt I.2a)-I.2c) (w zadaniu nr 1) - w wymiarze 15h przez inżyniera certyfikowanego przez producenta urządzeń

Termin realizacji zamówienia w zakresie dostawy: 30 dni od podpisania umowy.

Termin realizacji zamówienia w zakresie szkolenia: 6 miesięcy od podpisania umowy.

Miejsce dostawy zamówienia: siedziba Zamawiającego, Warszawa 00-928, ul. Chałubińskiego 4.

1. Wymagania szczegółowe:
2. Wykonawca musi być autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam być producentem przedmiotu zamówienia.
3. Dostarczony przedmiot zamówienia musi być:
	1. fabrycznie nowy, oraz
	2. pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, oraz
	3. objęty gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne
4. **Wielozadaniowy system zabezpieczeń sieciowych** musi spełniać następujące właściwości / umożliwiać realizację następujących funkcjonalności:
	1. System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
	2. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
	3. Urządzenie zabezpieczeń musi posiadać przepływność w ruchu full-duplex nie mniej niż 2 Gb/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1 Gb/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 250 000 jednoczesnych połączeń.
	4. System zabezpieczeń musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
	5. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność urządzenia zabezpieczeń przy włączonej identyfikacji aplikacji w ruchu full-duplex musi być nie mniejsza niż 2 Gb/s.
	6. Urządzenie zabezpieczeń musi być wyposażone w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 8 interfejsów optycznych (SFP).
	7. System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych. Musi istnieć możliwość jednoczesnej konfiguracji i pracy poszczególnych interfejsów sieciowych w różnych trybach w pojedynczej instancji systemu zabezpieczeń.
	8. Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
	9. Urządzenie musi mieć możliwość pracy w trybie transparentnym L1 (bez konieczności nadawania adresu IP) oraz pozwalać na tworzenie transparentnych subinterfejsów, które będą obsługiwały ruch z wybranych vlanów lub podsieci IP.
	10. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tabela routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
	11. System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
	12. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa.
	13. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
	14. System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
	15. System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
	16. System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
	17. System zabezpieczeń musi identyfikować co najmniej 1700 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, nie mniej niż: Skype, Gada-Gadu, Tor, BitTorrent, eMule.
	18. System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
	19. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama.
	20. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
	21. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
	22. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
	23. System zabezpieczeń musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez urządzenie.
	24. System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
	25. System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
	26. System zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
	27. Urządzenie zabezpieczeń musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznego systemu typu „Sand-Box” plików wykonywalnych (exe, dll) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 1 Gb/s w celu ochrony przed zagrożeniami typu zero-day. System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
	28. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, oba), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.
	29. Administrator musi mieć możliwość dostępu do systemu analizy plików wykonywalnych w celu sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
	30. System zabezpieczeń musi umożliwiać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.
	31. System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
	32. System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
	33. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
	34. System zabezpieczeń musi posiadać możliwość automatycznego pobierania listy stron WWW z zewnętrznego systemu w określonych przedziałach czasu i używania ich w politykach bezpieczeństwa.
	35. System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
	36. System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
	37. System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
	38. System zabezpieczeń musi posiadać możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
	39. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
	40. System zabezpieczeń musi posiadać możliwość uruchomienia modułu anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
	41. System zabezpieczeń musi posiadać możliwość uruchomienia modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
	42. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
	43. System zabezpieczeń musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
	44. System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
	45. System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
	46. System zabezpieczeń musi umożliwiać integrację funkcjonalności mapowania nazw użytkowników do używanych adresów IP z rozwiązaniami niestandardowymi (np. kontrolerami sieci WiFi) za pomocą dostępnego interfejsu API.
	47. Interfejs API musi być integralną częścią systemu zabezpieczeń umożliwiającą konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
	48. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
	49. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
	50. System zabezpieczeń musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS i Kerberos.
	51. System musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
	52. System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
	53. System zabezpieczeń zapewnia możliwość bezpiecznego zdalnego dostępu do chronionych zasobów w oparciu o standard SSL VPN bez konieczności stosowania dodatkowych licencji.
	54. System zabezpieczeń musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
	55. Urządzenie zabezpieczeń musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 100 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
	56. Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia.
	57. Urządzenie musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
	58. Urządzenie musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
	59. Urządzenie musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika na przestrzeni kilku ostatnich dni.
	60. Urządzenie musi mieć możliwość generowania raportu na temat aktywności sieci typu Botnet wykrywanych przez system zabezpieczeń.
	61. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
	62. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.
	63. Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 12 miesięcy z możliwością przedłużenia o co najmniej 12 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu w ciągu 1 dnia roboczego (od momentu potwierdzenia awarii), dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Wymagany czas usunięcia awarii w okresie gwarancji (lub dostarczenia i produkcyjnego uruchomienia urządzenia zastępczego o zbliżonych parametrach): następny dzień roboczy po zgłoszeniu.
	64. Dostawca przedstawi też zaświadczenie wystawione przez przedstawicielstwo producenta na Polskę stwierdzające, że sprzęt przeznaczony dla Zamawiającego pochodzić będzie z autoryzowanej sieci sprzedaży na terenie Polski, oraz że Dostawca posiada wymagane autoryzacje do odsprzedaży i serwisowanie sprzętu.
	65. Dostawca musi zatrudniać minimum 2 certyfikowanych przez producenta inżynierów wsparcia technicznego przeszkolonych w zakresie przedmiotowego sprzętu i oprogramowania
5. **Przełączniki sieci typu LAN PoE warstwy 2 o stałej konfiguracji z możliwością pracy w stosie** muszą spełniać następujące właściwości / umożliwiać realizację następujących funkcjonalności:
	1. Wysokość urządzenia: 1U
	2. Przystosowany do montowania w szafie rackowej
	3. Ilość portów dostępowych Ethernet 10/100/1000 Auto‐MDI/MDIX: min. 48
	4. Wszystkie porty dostępowe muszą obsługiwać standard 802.3af (Power over Ethernet) oraz 802.at (Power over Ethernet+). Przełącznik musi udostępniać 15.4 W na każdym porcie dostępowym jednocześnie
	5. Ilość portów uplink 10 Gigabit Ethernet SFP+: min. 4
	6. Korzystanie z portów uplink nie może powodować wyłączenia portów dostępowych 10/100/1000. Wymiana modułu uplink nie może wymagać wyłączenia przełącznika. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet
	7. Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 6 urządzeń. Dopuszczalne jest podłączanie do stosu portami uplink 10 Gb/s. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup’u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master
	8. Przełącznik musi posiadać wbudowany zasilacz AC.
	9. Urządzenie musi posiadać wentylator – z przepływem powietrza od przodu do tyłu.
	10. Urządzenie musi posiadać panel LCD z przyciskami, pozwalający na wykonywanie podstawowych czynności związanych z zarządzaniem (adresacja IP, reset)
	11. Musi istnieć możliwość podłączenia zewnętrznego redundantnego źródła zasilania.
	12. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out‐of‐band)
	13. Pamięci Flash: min. 1GB
	14. Pamięci DRAM: min. 1GB
	15. Zarządzanie urządzeniem musi odbywać się za pośrednictwem: linii komend (CLI) przez port konsoli oraz telnet/ssh oraz telnet/ssh na interfejsie OoB
	16. Urządzenie posiada możliwość włączenia/wyłączenia dostępności zarządzania przez porty niededykowane.
	17. Architektura „non‐blocking” uniemożliwiająca blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów
	18. Wydajność przełączania w warstwie 2: min. 175 Gb/s oraz min. 130 milionów pakietów na sekundę
	19. Ilość obsługiwanych adresów MAC: min. 16 000
	20. Obsługa ramek Jumbo (9216 bajtów)
	21. Obsługa sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4096
	22. Obsługa sieci VLAN opartych o porty fizyczne (port‐based) i adresy MAC (MAC‐based)
	23. Obsługa automatycznej konfiguracji sieci VLAN poprzez protokół MVRP
	24. Obsługa agregowania połączeń zgodne z IEEE 802.3ad min. 32 grupy oraz co najmniej 8 portów w grupie
	25. Obsługa protokółu Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D i 802.1w
	26. Obsługa protokołu Multiple Spanning Tree zgodnie z IEEE 802.
	27. Obsługa protokołów LLDP i LLDP‐MED
	28. Obsługa rutingu między sieciami VLAN – ruting statyczny, oraz protokół rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 8 000
	29. Obsługa funkcji IGMP Snooping (v1, v2, v3).
	30. Urządzenie musi posiadać mechanizmy priorytetyzowania dla ruchu wchodzącego i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
	31. Obsługa filtrowania ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2‐4. Urządzenie musi realizować sprzętowo nie mniej niż 1300 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
	32. Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping
	33. Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
	34. Obsługa protokołu SNMP (wersje 2 i 3), oraz grupy RMON 1, 2, 3, 9.
	35. Funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
	36. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną, a poszczególne moduły muszą działać niezależnie. W szczególności działanie modułu przekazywania pakietów (odpowiedzialnego za przełączanie pakietów) musi być niezależne od poprawności funkcjonowania modułu rutingu IP (odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem).
	37. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
	38. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
	39. Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 12 miesięcy z możliwością przedłużenia o co najmniej 12 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu w ciągu 1 dnia roboczego (od momentu potwierdzenia awarii), dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Wymagany czas usunięcia awarii w okresie gwarancji (lub dostarczenia i produkcyjnego uruchomienia urządzenia zastępczego o zbliżonych parametrach): następny dzień roboczy po zgłoszeniu.
	40. Dostawca przedstawi też zaświadczenie wystawione przez przedstawicielstwo producenta na Polskę stwierdzające, że sprzęt przeznaczony dla Zamawiającego pochodzić będzie z autoryzowanej sieci sprzedaży na terenie Polski, oraz że Dostawca posiada wymagane autoryzacje do odsprzedaży i serwisowanie sprzętu.
	41. Dostawca musi zatrudniać minimum 2 certyfikowanych przez producenta inżynierów wsparcia technicznego przeszkolonych w zakresie przedmiotowego sprzętu i oprogramowania.
6. **Wkładki typu SFP+** (kompatybilne z dostarczanymi w pkt 4 przełącznikami sieci LAN PoE warstwy 2 o stałej konfiguracji z możliwością pracy w stosie) muszą spełniać następujące właściwości / umożliwiać realizację następujących funkcjonalności:
	1. zgodność z 10GBASE‐SR/SW
	2. spełnienie wymagań RoHS zgodnie z dyrektywą 2002/95/EC i notą AN‐2038
	3. Transmisja danych z prędkością od 9,95 do 10,3Gb/s oraz 1,25Gb/s,
	4. Zasięg do 300m przy użyciu światłowodów wielomodowych
	5. Cyfrowe funkcje diagnostyczne
	6. Praca w zakresie temperatur (od 0°C do +70°C),
	7. W pełni metalowa obudowa ograniczająca interferencje elektromagnetyczne
	8. Gwarancja dostawcy współpracy z oferowanymi modułami uplink przełączników

**Część 2 (zadanie nr 2).**

**ZAKUP I DOSTARCZENIE DYSKÓW DO MACIERZY DYSKOWEJ.**

1. Przedmiotem Zamówienia jest **zakup i dostarczenie dysków do macierzy IBM System Storage DS3400** (wymiana wyeksploatowanych lub uszkodzonych dysków):
2. **1 TB SATA PN 43W7633 lub równoważny** – 4 szt.
3. **450 GB SAS PN 42D0520 lub równoważny** – 4 szt.

Kryterium równoważności w obu w/w. asortymentach – taka sama (co oryginalnie wymagane):

1. funkcjonalności i właściwości
2. parametry techniczne, sprzętowe oraz przesyłowe
3. ergonomia użytkowania
4. architektura wewnętrzna
5. współkompatybilność z macierzą posiadaną przez Zamawiającego

Termin realizacji zamówienia: 14 dni od podpisania umowy.

Miejsce dostawy zamówienia: siedziba Zamawiającego, Warszawa 00-928, ul. Chałubińskiego 4.

1. Wymagania szczegółowe:
2. Wykonawca musi być autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam być producentem przedmiotu zamówienia.
3. Dostarczony przedmiot zamówienia musi być:
	1. fabrycznie nowy, oraz
	2. pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, oraz
	3. objęty gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne

Załącznik nr 2

**Wzór umowy**

w postępowaniu na zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych
wraz z wsparciem przy wdrożeniu i szkoleniem, zakup i dostarczenie przełączników warstwy drugiej
wraz z osprzętem i wsparciem przy wdrożeniu oraz zakup i dostarczenie dysków do macierzy

**Skarbem Państwa - Urzędem Transportu Kolejowego**

z siedzibą w Warszawie (kod: 00‐928) przy ul. Chałubińskiego 4 reprezentowanym przez:

………………………………….. ‐ ……………………………………

zwanym dalej **Zamawiającym**

a

**……………………………………………………………………………………………………….**

reprezentowanym przez:

**………………………………. ‐ ……………………………….**

zwanego dalej **Wykonawcą**.

W związku z przeprowadzonym postępowaniem zamówieniowym, w trybie przetargu nieograniczonego, realizowanym na podstawie zapisów Ustawy PZP, strony zawarły następująca umowę:

* 1. Przedmiotem umowy jest sprzedaż i dostarczenie (wraz z przeszkoleniem z użytkowania) przez Wykonawcę Zamawiającemu przedmiotu zamówienia, zgodnego ze szczegółowym opisem, w ilości, na zasadach oraz według cen jednostkowych, określonych w załączniku nr 1 do umowy.
	2. Sprzedaż oraz dostarczenie przedmiotu umowy, określonego w §1 ust. 1 niniejszej umowy musi odbyć się w ciągu …………………. od dnia zawarcia niniejszej umowy.
	3. Wykonawca zawiadomi Zamawiającego o gotowości do realizacji dostawy faksem lub pocztą elektroniczną (wg danych określonych w §7 ust 1 niniejszej umowy). Wykonawca dostarczy przedmiot umowy do miejsca wskazanego przez Zamawiającego w terminie ustalonym z Zamawiającym, jednakże termin ten musi mieścić się w terminie określonym w §1 ust. 2 niniejszej umowy.
	4. Przedmiot dostawy musi charakteryzować się wysoką jakością wykonania i – o ile jest to wymagane przepisami prawa - musi posiadać aktualną deklarację zgodności: z Polską Normą lub Aprobatą Techniczną lub innymi, wymaganymi przepisami prawa normatywami (w tym np. deklaracja CE – o ile jest wymagana). Wykonawca, do upływu terminu określonego w §1 ust. 2 niniejszej umowy, dostarczy bez wezwania przez Zamawiającego – wszelkie wymagane prawem certyfikaty, deklaracje zgodności lub inne dokumenty, potwierdzające spełnienie przez przedmiot zamówienia wszelkich wymaganych prawem normatywów. W przypadku braku aktualnych a wymaganych prawem deklaracji zgodnych z Polską Normą lub Aprobatą Techniczną, itp. itd., Zamawiający może rozwiązać Umowę z winy leżącej po stronie Wykonawcy - §4 ust 1 niniejszej umowy stosuje się odpowiednio.
	5. Po poprawnym zrealizowaniu dostawy, Zamawiający wystawi Wykonawcy potwierdzenie odbioru. Moment wystawienia potwierdzenia odbioru dostawy uważany będzie za moment jej realizacji. Zamawiający ma prawo nie wystawić potwierdzenia odbioru tylko w razie stwierdzenia niepoprawności realizacji dostawy, podając w sposób pisemny uzasadnienie takiej decyzji.
	6. Podpisane przez osobę określoną w §7 ust. 1 niniejszej umowy potwierdzenia odbioru dostawy jest podstawą do wystawienia przez Wykonawcę faktury VAT za daną dostawę.
	7. Wykonawca oświadcza, iż przedmiot zamówienia, określony w §1 ust. 1 zrealizuje w sposób terminowy, dochowując należytej staranności wymaganej w profesjonalnym obrocie, biorąc pod uwagę zawodowy sposób wykonywania działalności przez Wykonawcę w tym zakresie.
	8. Wykonawca udziela …………….. miesięcznego okresu gwarancji na przedmiot dostawy, licząc od daty dostarczenia danej dostawy i wystawienia protokołu odbiorczego przez Zamawiającego (dokumentem potwierdzającym powyższą gwarancję jest przede wszystkim niniejsza umowa).
	9. W okresie gwarancji Wykonawca usunie wszelkie wady fizyczne przedmiotu umowy wykryte w trakcie eksploatacji albo dostarczy przedmiot wolny od wad w ciągu 14 dni kalendarzowych od dnia otrzymania zawiadomienia Zamawiającego (reprezentowanego przez osobę określoną w §7 ust. 1 niniejszej umowy) za pomocą faksu lub poczty elektronicznej o istnieniu wad.
	10. (Dotyczy wyłącznie części nr 1 w zakresie dostarczanego wielozadaniowego systemu zabezpieczeń sieciowych) Niezależnie od powyższego:
		1. Wykonawca musi zatrudniać minimum 2 certyfikowanych przez producenta inżyniera wsparcia technicznego przeszkolonego w zakresie przedmiotowego sprzętu i oprogramowania; oraz
		2. Wykonawca musi zapewnić Zamawiającemu 50 godzin w ciągu 12 miesięcy od podpisania umowy wsparcia przy wdrożeniu i konfiguracji dostarczanego wielozadaniowego systemu zabezpieczeń sieciowych. Szczegółowa realizacja powyższego odbywać się będzie w terminach i na zasadach uzgodnionych z Zamawiającym bezzwłocznie po podpisaniu umowy, oraz
		3. Wykonawca zapewni autoryzowane przez producenta systemu szkolenie z użytkowania dostarczanego wielozadaniowego systemu zabezpieczeń sieciowych dla jednego administratora zamawiającego w wymiarze min 35 godzin. Termin szkolenia w ciągu 6 miesięcy od dnia podpisania umowy - ustalony z Zamawiającym na terenie Warszawy.
	11. (Dotyczy wyłącznie części nr 1 w zakresie dostarczanego sprzętu i osprzętu sieciowego IT: przełączników sieci typu LAN, wkładek typu SFP+ oraz patchcordu światłowodowego) Niezależnie od powyższego:
		1. Wykonawca musi zatrudniać minimum 2 certyfikowanego przez producenta inżyniera wsparcia technicznego przeszkolonego w zakresie przedmiotowego sprzętu i oprogramowania; oraz
		2. Wykonawca musi zapewnić Zamawiającemu 15 godzin w ciągu 12 miesięcy od podpisania umowy wsparcia przy wdrożeniu i konfiguracji dostarczanego sprzętu i osprzętu sieciowego IT: przełączników sieci typu LAN, wkładek typu SFP+ oraz patchcordu światłowodowego. Szczegółowa realizacja powyższego odbywać się będzie w terminach i na zasadach uzgodnionych z Zamawiającym bezzwłocznie po podpisaniu umowy;
	12. Wynagrodzenie za poprawną i terminową realizację dostaw, o których mowa w §1 ust. 1 niniejszej umowy, strony ustalają na kwotę netto ………. zł (*słownie: ……… zł*), plus podatek VAT w wysokości ……..%, co łącznie stanowi kwotę brutto ………. zł (*słownie: ……… zł*), z zastrzeżeniem §5 ust. 4 niniejszej umowy.
	13. Wynagrodzenie określone w §3 ust. 1 niniejszej umowy, zawiera wszelkie koszty, jakie związane są z dostawą przedmiotu zamówienia, określonego w §1 ust. 1 niniejszej umowy, w tym m.in. koszty transportu, załadunku, rozładunku do miejsca wskazanego przez Zamawiającego, ubezpieczenia itp. itd.
	14. Wykonawca wystawi fakturę VAT za poprawnie zrealizowaną dostawę po otrzymaniu od Zamawiającego potwierdzenia odbioru dostawy, o którym mowa w §1 ust. 5-6 niniejszej umowy. Wynagrodzenie określone na fakturze płatne będzie na konto Wykonawcy wskazane na fakturze, w terminie do 14 dni od daty doręczenia Zamawiającemu faktury.
	15. Wykonawca wystawiając fakturę obowiązany jest w jej treści powołać się na numer umowy.
	16. Niezależnie od przypadków przewidzianych w kodeksie cywilnym, Zamawiający może od niniejszej umowy odstąpić w całości lub części:
		1. w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy;
		2. w przypadku opóźnienia się z rozpoczęciem lub wykonaniem umowy w taki sposób, iż nie jest prawdopodobnym wykonanie przedmiotu umowy w ustalonym terminie, określonym w §1 ust 2 niniejszej umowy;
		3. w przypadku, gdy majątek Wykonawcy lub służące mu prawa lub wierzytelności zostaną zajęte;
		4. utraty przez Zamawiającego źródła finansowania zamówienia w całości lub części, a także w przypadku przesunięcia źródeł finansowania zamówienia;
	17. Odstąpienie od umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia. Z prawa odstąpienia, o jakim mowa w niniejszej umowie Zamawiający można skorzystać w terminie do 60 dni od powzięcia wiadomości o zdarzeniach stanowiących podstawę odstąpienia. W przypadku określonym w §4 ust. 1 pkt 1) termin do skorzystania przez Zamawiającego z prawa odstąpienia wynosi do 30 dni.
	18. W przypadku odstąpienia z przyczyn leżących po stronie Wykonawcy, zapisy §5 ust. 1 oraz ust. 4-5 niniejszej umowy - stosuje się.
	19. Za odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20% wynagrodzenia netto, określonego w §3 ust. 1 niniejszej umowy.
	20. Za opóźnienie w realizacji dostawy, w stosunku do terminu określonego na podstawie §1 ust. 2 niniejszej umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,5% wynagrodzenia określonego w §3 ust. 1 niniejszej umowy za każdy kalendarzowy dzień opóźnienia. Zapłata kary umownej nie zwalnia Wykonawcy od obowiązku realizacji danej dostawy.
	21. Wykonawca zapłaci Zamawiającemu karę umowną za opóźnienie w usunięciu wad lub w wymianie towaru wadliwego na niewadliwy – w rozumieniu §2 ust. 2 niniejszej umowy - w wysokości 0,5% wynagrodzenia netto wadliwej dostawy za każdy kalendarzowy dzień opóźnienia. Zapłata kary umownej nie zwalnia Wykonawcy od obowiązku realizacji uprawnień Zamawiającego wynikających z tytułu gwarancji.
	22. W przypadku naliczenia przez Zamawiającego kar umownych wg zasad określonych w niniejszym paragrafie, Zamawiający wystawi Wykonawcy stosowną notę obciążeniową. Wynagrodzenie wypłacane Wykonawcy wg zasad określonych w §3 niniejszej umowy może zostać pomniejszone o wartość not obciążeniowych, na co Wykonawca wyraża zgodę.
	23. W przypadku powstania szkód z tytułu niewykonania lub nienależytego wykonania umowy przewyższających wysokość kar umownych, określonych w niniejszym paragrafie, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania przenoszącego wysokość zastrzeżonych kar (odszkodowanie uzupełniające).
	24. Zamawiający przewiduje, w celu należytego wykonania przedmiotu umowy, możliwość zmiany jej postanowień w stosunku do treści oferty Wykonawcy, w tym zmianę: ostatecznego terminu wykonania przedmiotu umowy, zmianę przedmiotu umowy, zasad wypłaty wynagrodzenia, wysokości wynagrodzenia, sposobu odbioru towaru - o ile zostanie spełniony jeden z następujących warunków:
		1. w sytuacji zaistnienia siły wyższej
		2. gdy konieczność zmiany jest spowodowana zaistnieniem niezawinionych przez Wykonawcę lub/oraz Zamawiającego okoliczności, których nie można było przy dołożeniu należytej staranności przewidzieć w chwili zawarcia umowy, a które uniemożliwiają prawidłowe wykonanie przedmiotu umowy w terminie określonym w § 1 ust. 2 niniejszej umowy.
		3. utraty przez Zamawiającego źródła finansowania zamówienia w całości lub części, a także w przypadku przesunięcia źródeł finansowania zamówienia.
		4. zmian po zawarciu umowy przepisów prawa lub wprowadzenia nowych przepisów prawa lub zmiany lub wprowadzenia nowej bezwzględnie obowiązującej normy powodującej konieczność zmiany, modyfikacji lub odstępstwa w odniesieniu do przedmiotu zamówienia;
		5. zmiana ustawowej stawki podatku VAT lub innych obiektywnych obciążeń podatkowych;
	25. Wystąpienie którejkolwiek z wymienionych w §6 ust. 1 niniejszej umowy okoliczności nie stanowi bezwzględnego zobowiązania Zamawiającego do dokonania takich zmian, ani nie może stanowić podstawy roszczeń Wykonawcy do ich dokonania.
	26. Ewentualna zmiana umowy nastąpi z uwzględnieniem wpływu, jaki wywiera wystąpienie okoliczności uzasadniającej modyfikację na dotychczasowy kształt zobowiązania umownego.
	27. Niezależnie od zapisów §6 ust. 1 niniejszej umowy, ceny jednostkowe określone w załączniku nr 1 do umowy (oferta Wykonawcy), nie mogą ulec zmianie na niekorzyść Zamawiającego przez okres obowiązywania umowy.
	28. Krzysztof Rumniak jest osobą ze strony Zamawiającego odpowiedzialną za realizacje niniejszej umowy, w tym upoważnioną do kontaktów z Wykonawcą, w sprawach związanych z realizacją niniejszej umowy w czasie jej obowiązywania (w tym – w okresie gwarancyjnym). Dane teleadresowe: telefon stacjonarny: 22-630-18-85 telefon komórkowy: 603-780-171, poczta mailowa: krzysztof.rumniak@utk.gov.pl;
	29. ……………… jest osobą upoważnioną do kontaktów z Zamawiającym, w sprawach związanych z realizacją niniejszej umowy w czasie jej obowiązywania (w tym – w okresie gwarancyjnym). Dane teleadresowe: telefon stacjonarny: ……………………, telefon komórkowy: ……………….., poczta mailowa: ……………………….
	30. Zmiana osób określonych w §7 ust. 1 oraz ust. 2 niniejszej umowy, wymaga bezzwłocznego zawiadomienia drugiej strony umowy w sposób pisemny lub faksem, oraz nie wymaga aneksu do niniejszej umowy.
	31. Wykonawca nie może dokonać cesji swojej wierzytelności wynikającej z niniejszej umowy na rzecz osoby trzeciej bez zgody Zamawiającego wyrażonej na piśmie.
	32. Wszelkie zmiany do niniejszej umowy wymagają formy pisemnej pod rygorem nieważności, z zastrzeżeniem §7 ust. 3 niniejszej umowy.
	33. Sprawy sporne wynikające z treści niniejszej umowy rozstrzygane będą przez Sąd właściwy ze względu na siedzibę Zamawiającego.
	34. Dla potrzeb wzajemnych rozliczeń Wykonawca oświadcza, że jest płatnikiem podatku od towarów i usług VAT
		+ 1. NIP – …………………
			2. REGON: ………………
	35. W sprawach nie uregulowanych treścią umowy zastosowanie mają przepisy Kodeksu cywilnego.
	36. Niniejsza umowa sporządzona została w 3 jednobrzmiących egzemplarzach, 2 dla Zamawiającego, 1 dla Wykonawcy.
	37. Załącznikami do niniejszej umowy są:
		1. Opis Przedmiotu Zamówienia
		2. Formularz opisowo-cenowy (oferta Wykonawcy).
		3. Wypis z KRS lub Centralnej Ewidencji i Informacji Działalności Gospodarczej Wykonawcy (wraz z ewentualnymi pełnomocnictwami), wskazujący na możliwość wiążącego zawarcia niniejszej umowy przez osobę (osoby) reprezentującą (reprezentujące) Wykonawcę.
		4. Kopie certyfikatów inżynierów wsparcia technicznego (dotyczy wyłącznie części nr 1)

**ZAMAWIAJĄCY WYKONAWCA**

**Załącznik** **nr** **3**

……………………………………. pieczęć Wykonawcy

Nazwa Wykonawcy: ………………………………………………………………………………..………………………

Siedziba Wykonawcy: ………………………………………………………………………………………………………

REGON Wykonawcy: …………………………………………………………………………………….…………………

NIP Wykonawcy: ……………………………………………………………………………………………………….…...

Osoba uprawniona do kontaktu z Zamawiającym:

imię i nazwisko: …………………………….……… stanowisko: ………………………………………..……….………

nr telefonu oraz faksu …………………………………………… adres mailowy …………………….…………………

**FORMULARZ OFERTOWY**

Do: **Urzędu Transportu Kolejowego, 00‐928 Warszawa, ul. Chałubińskiego 4**

Nawiązując do zaproszenia do składania ofert w trybie przetargu nieograniczonego o wartości poniżej 134.000 euro na:

**na zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych wraz z wsparciem przy wdrożeniu i szkoleniem, zakup i dostarczenie przełączników warstwy drugiej wraz z osprzętem i wsparciem przy wdrożeniu oraz zakup i dostarczenie dysków do macierzy (Nr: BAF-2311-……../2014), oferujemy wykonanie przedmiotu zamówienia w zakresie:**

**Część 1 (zadanie nr 1). ZAKUP I DOSTARCZENIE WIELOZADANIOWEGO SYSTEMU ZABEZPIECZEŃ SIECIOWYCH WRAZ Z WSPARCIEM PRZY WDROŻENIU I SZKOLENIEM, ORAZ ZAKUP I DOSTARCZENIE SPRZĘTU I OSPRZĘTU SIECIOWEGO IT WRAZ Z WSPARCIEM PRZY WDROŻENIU.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Ilość** | **Cena pojedynczego asortymentu netto** | **Cena sumaryczna asortymentu netto** | **Podatek VAT** | **Cena sumaryczna asortymentu brutto** |
| 1. Zakup i dostarczenie wielozadaniowego systemu zabezpieczeń sieciowych Model/typ: ………………………………………………… Producent: …..…………………………………………… | 1 szt. |   |   |   |   |
| 2. Wsparcie przy wdrożeniu wielozadaniowego systemu zabezpieczeń sieciowych (pkt 1) przez inżyniera certyfikowanego przez producenta systemu | 50 h |   |   |   |   |
| 3. Autoryzowane przez producenta systemu szkolenie z użytkowania systemu (pkt 1) na terenie Warszawy dla jednego administratora Zamawiającego w min wymiarze 35 h | 1 osoba |   |   |   |   |
| 4. Zakup i dostarczenie przełączników sieci typu LAN PoE warstwy 2 o stałej konfiguracji z możliwością pracy w stosie Model/typ: ………………………………………………… Producent: …..…………………………………………… | 3 szt. |   |   |   |   |
| 5. Zakup i dostarczenie wkładki typu SFP+ Model/typ: …………………………………………………Producent: …..…………………………………………… | 6 szt. |   |   |   |   |
| 6. Zakup i dostarczenie patchcordu światłowodowego typu LC‐LC, 50/125um, o długości 2 mModel/typ: …………………………………………………Producent: …..…………………………………………… | 6 szt. |   |   |   |   |
| 7. Wsparcie przy wdrożeniu urządzeń określonych w pkt 4-6, przez inżyniera certyfikowanego przez producenta urządzeń | 15 h |   |   |   |   |
|  | Cena oferty w zakresie zadania nr 2 brutto: |   |

**Akceptujemy: Terminy i zasady płatności oraz zasady gwarancji, określone w SIWZ.**

**Część 2 (zadanie nr 2). ZAKUP I DOSTARCZENIE DYSKÓW DO MACIERZY DYSKOWEJ.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Ilość** | **Cena pojedynczego asortymentu netto** | **Cena sumaryczna asortymentu netto** | **Podatek VAT** | **Cena sumaryczna asortymentu brutto** |
| 1. Zakup i dostarczenie dysków do macierzy IBM System Storage DS3400: 1 TB SATA PN 43W7633 lub równoważny Model/typ: ………………………………………………… Producent: …..…………………………………………… | 4 szt. |   |   |   |   |
| 2. Zakup i dostarczenie dysków do macierzy IBM System Storage DS3400: 450 GB SAS PN 42D0520 lub równoważny – 4 szt. Model/typ: …………………………………………………Producent: …..…………………………………………… | 4 szt. |   |   |   |   |
|  | Cena oferty w zakresie zadania nr 2 brutto: |   |

**Akceptujemy: Terminy i zasady płatności oraz zasady gwarancji, określone w SIWZ.**

\* - Wykonawca może złożyć ofertę na dowolną liczbę zadań. W przypadku braku oferty na dane zadanie, należy pola cenowe tego zadania przekreślić lub pozostawić niewypełnione.

W związku ze złożoną ofertą:

1. Oświadczamy, iż dokładając należytą staranność, zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia wraz ze Wzorem Umowy oraz Opisem Przedmiotu Zamówienia ‐ i nie wnosimy do nich zastrzeżeń, oraz że zdobyliśmy konieczne informacje do przygotowania oferty.

2. Oświadczamy, że Wzór Umowy, stanowiący załącznik nr 2 do specyfikacji istotnych warunków zamówienia, został przez nas zaakceptowany w całości i bez zastrzeżeń i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na zaproponowanych warunkach w określonym przez Zamawiającego terminie.

3. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez czas wskazany w specyfikacji istotnych warunków zamówienia.

4. Oświadczamy, iż za wyjątkiem informacji i dokumentów zawartych na kartkach opatrzonych napisem **„POUFNE”** na stronach: do …………….. do ………………… (określa Wykonawca – w przypadku pełnej jawności – prosimy skreślić lub nie wypełniać) niniejsza oferta oraz wszelkie załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

5. Ofertę niniejszą składamy na ….................. kolejno ponumerowanych kartkach.

6. Oświadczenie Wykonawcy o powierzeniu części zamówienia podwykonawcom - części zamówienia, których wykonanie wykonawca zamierza powierzyć podwykonawcom (w przypadku niepowierzana – prosimy o niewypełnianie niżej określonych punktów):

 a) …………………………..

 b) …………………………..

7. W zakresie zapisów art. 24 ust. 2 pkt 5 Ustawy PZP – oświadczamy, iż:

- nie należymy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 Ustawy PZP\*,

- należymy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 Ustawy PZP\*.

(\* - niewłaściwe skreślić)

W przypadku przynależności Wykonawcy do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 Ustawy PZP, Wykonawca składa wraz z ofertą - listę podmiotów należących do grupy kapitałowej.

Lista podmiotów należących do grupy kapitałowej (w przypadku braku konsumpcji przesłanki z art. 24 ust 2 pkt 5 Ustawy PZP – prosimy o niewypełnianie niżej określonych punktów):

 a) …………………………..

 b) …………………………..

**OŚWIADCZENIE WYKONAWCY**

W imieniu Wykonawcy, tj. (nazwa – firma Wykonawcy) ………………………………………………………, biorąc pod uwagę odpowiedzialność cywilną oraz karną za złożenie fałszywego oświadczenia ‐ oświadczam, iż:

1) w/w. Wykonawca nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 Ustawy PZP, tj. m.in.:

a) nie figuruje w Kartotece Podmiotów Zbiorowych Krajowego Rejestru Karnego, oraz o nie figuruje w Kartotece Karnej Krajowego Rejestru Karnego, tj. w zakresie określonym w art. 24 ust. 1 pkt 1‐11 Ustawy PZP oraz

b) nie zalega z opłacaniem podatków (Urząd Skarbowy), lub uzyskał przewidziane prawem zwolnienie,

odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu, oraz

c) nie zalega z opłacaniem składek na ubezpieczenia zdrowotne i społeczne (Zakład Ubezpieczeń Społecznych lub Kasa Rolniczego Ubezpieczenia Społecznego), lub uzyskał przewidziany prawem zwolnienia, odroczenia lub rozłożenia na raty zaległych płatności lub wstrzymaniu w całości wykonania decyzji właściwego organu

2) w/w. Wykonawca nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 2 Ustawy PZP

3) w/w. Wykonawca posiada uprawnienie do wykonywania określonej działalności i czynności będących przedmiotem niniejszego zamówienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień; posiada niezbędną wiedzę i doświadczenie (do wykonania zamówienia), tj. Wykonawca:

- **jest autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam jest producentem przedmiotu zamówienia**.

- **zatrudnia minimum 2 certyfikowanych przez producenta inżynierów wsparcia technicznego prze-szkolonych w zakresie przedmiotowego sprzętu i oprogramowania.**

4) w/w. Wykonawca jest uprawniony do wykonywania działalności gospodarczej w zakresie realizacji przedmiotu zamówienia w niniejszym postepowaniu.

5) oferowany przedmiot zamówienia spełnia warunki określone w Opisie Przedmiotu Zamówienia z za-łącznika nr 1 do SIWZ, w tym, w szczególności – dostarczony przedmiot zamówienia jest fabrycznie nowy, pochodzi z oficjalnego kanału sprzedaży producenta na rynek polski, oraz objęty jest gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne, oraz iż oferowany przedmiot zamówienia spełnia warunki zgodności wynikające z wszelkich, powszechnie obowiązujących, określonych przepisami prawa norm na terenie Rzeczpospolitej Polskiej, w tym za-kresie;;

Do oferty załączono:

* + - 1. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
			2. Dokument potwierdzający, iż Wykonawca jest: autoryzowanym partnerem handlowym producenta przedmiotu zamówienia lub sam jest producentem przedmiotu zamówienia.
			3. Ilustrowane foldery producenta, rysunki, opisy techniczne, potwierdzające, że oferowany przedmiot zamówienia spełnia minimalne parametry określone przez Zamawiającego w Opisie Przedmiotu Zamówienia w zał. nr 1 do SIWZ.
			4. Pełnomocnictwo do reprezentacji Wykonawcy (jeśli upoważnienie do podpisania niniejszej oferty nie wynika w odpisu z właściwego rejestru.

**……………………………………………..**

(miejscowość, data)

**……………………………………………..**

(podpis z pieczątką imienną, lub podpis czytelny osoby uprawnionej do reprezentowania Wykonawcy)