Projekt nr **POIR.01.01.01-00-0180/22** pn.: „**Centrum monitorowania instalacji przemysłowych w podziemnych zakładach górniczych i wykrywania cyberzagrożeń”** realizowany w ramach Poddziałania 1.1.1 Programu Operacyjnego Inteligentny Rozwój 2014-2020 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego

Postępowanie nr 07/2023

Specyfikacja warunków zamówienia (SWZ) w ramach projektu POIR.01.01.01-00-0180/22 „Centrum monitorowania instalacji przemysłowych w podziemnych zakładach górniczych i wykrywania cyberzagrożeń”.

Zadanie nr 1 – zakup przełącznika sieciowego LAN do szafy RACK 19” – 1 szt.

Zadanie nr 2 – zakup przełączników sieciowych LAN do szafy RACK 19” – 2 szt.

Zadanie nr 3 – zakup przełącznika sieciowego LAN na szynę DIN TH35mm – 1 szt.

Zadanie nr 4 – zakup przełączników sieci LAN na szynę DIN TH35mm – 4 szt.

Zadanie nr 5 – zakup zapory sieciowej nowej generacji (NGFW) do szafy RACK 19” – 1 szt.

Zadanie nr 6 – zakup urządzenia do podstawowych pomiarów i weryfikacji światłowodowych sieci optycznych – 1szt.

1. Wstęp.

1.1. Zamawiający.

JSW IT Systems Spółka z o.o.
44-330 Jastrzębie-Zdrój, ul. Armii Krajowej 56

Tel: 32 700 27 10
Fax: 32 476 11 85
e-mail: firma@jswits.pl

NIP: 633-19-81-130
Regon: 276202273
KRS: 0000083839
BDO: 000154071

1.2. Informacje ogólne.

Na potrzeby niniejszego postępowania nie mają zastosowania przepisy ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (tj. Dz. U. z 2022 r. poz. 1710 z późn. zm.).

JSW IT Systems Spółka z o.o. zaprasza do składania ofert w postępowaniu prowadzonym zgodnie z zasadą konkurencyjności w rozumieniu Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 a także zgodnie z Regulaminem wyboru najkorzystniej oferty obowiązującym w JSW IT Systems Sp. z o.o. w trybie przetargu nieograniczonego. Regulamin dostępny na stronie internetowej https://www.jswits.pl/ogloszenia/zamowienia.
Wykonawca może złożyć ofertę częściową na wybrane przez siebie kompletne Zadanie.
Ceny w złożonej ofercie są ostateczne i nie podlegają negocjacjom.

W szczególnie uzasadnionych przypadkach Zamawiający ma prawo zmiany treści SWZ. Zmiana może nastąpić w każdym czasie, przed upływem terminu składania ofert. W przypadku wprowadzenia takiej zmiany, informacja o tym zostanie niezwłocznie przekazana w formie aktualizacji SWZ.

Zamawiający zastrzega sobie prawo do unieważnienia postępowania w każdym czasie, w szczególności Zamawiający może unieważnić postępowanie w całości bądź w części, jeżeli środki, które Zamawiający zamierzał przeznaczyć na sfinansowanie zamówienia nie zostały mu przyznane.

2. Opis przedmiotu zamówienia.

2.1. Przedmiot zamówienia.

Przedmiotem zamówienia jest dostawa urządzeń opisanych zgodnie z wymaganiami zawartymi dla poszczególnych zadań w Załączniku nr 1.

Zadanie nr 1. Zakup przełącznika sieciowego LAN do szafy RACK 19” – 1 szt.
Opis przedmiotu zamówienia zawiera Załącznik nr 1 Zadanie 1
Wspólny Słownik Zamówień:
- kody CPV: 32420000-3
Termin realizacji zadania nr 1: 30.06.2023 r.

Zadanie nr 2. Zakup przełączników sieciowych LAN do szafy RACK 19” – 2 szt.

Opis przedmiotu zamówienia zawiera Załącznik nr 1 Zadanie 2
Wspólny Słownik Zamówień:
- kod CPV: 32420000-3
Termin realizacji zadania nr 2: 30.06.2023 r.

Zadanie nr 3. Zakup przełącznika sieciowego LAN na szynę DIN TH35mm – 1 szt.
Opis przedmiotu zamówienia zawiera Załącznik nr 1 Zadanie 3
Wspólny Słownik Zamówień:
- kod CPV: 32420000-3
Termin realizacji zadania nr 3: 30.06.2023 r.

Zadanie nr 4. Zakup przełączników sieci LAN na szynę DIN TH35mm – 4 szt.
Opis przedmiotu zamówienia zawiera Załącznik nr 1 Zadanie 4
Wspólny Słownik Zamówień:
- kod CPV: 32420000-3
Termin realizacji zadania nr 4: 30.06.2023 r.

Zadanie nr 5. Zakup zapory sieciowej nowej generacji (NGFW) do szafy RACK 19” – 1 szt.
Opis przedmiotu zamówienia zawiera Załącznik nr 1 Zadanie 5
Wspólny Słownik Zamówień:
- kod CPV: 32413100-2
Termin realizacji zadania nr 5: 30.06.2023 r.

Zadanie nr 6. Zakup urządzenia do podstawowych pomiarów i weryfikacji światłowodowych sieci optycznych – 1szt.
Opis przedmiotu zamówienia zawiera Załącznik nr 1 Zadanie 6
Wspólny Słownik Zamówień:
- kod CPV: 38540000-2
Termin realizacji zadania nr 6: 30.06.2023 r.

2.2. Opis kosztów.

W celu uzyskania podstaw do rzetelnej oceny ofert złożona przez Wykonawcę oferta winna uwzględniać wszystkie koszty niezbędne do realizacji poszczególnych prac zgodnie z wymaganiami określonymi w niniejszym SWZ. Złożona oferta ma być ostateczna i nie będzie podlegać negocjacjom.

3. Instrukcja dla Wykonawcy.

3.1. Opis sposobu przygotowania ofert.

1. Oferta musi:
   a) być sporządzona w języku polskim, w jednym egzemplarzu;
   b) zawierać datę sporządzenia;
   c) zawierać adres lub siedzibę Wykonawcy, numer telefonu, numer NIP;
   d) być podpisana czytelnie przez Wykonawcę zgodnie z zasadami reprezentacji;
   e) zawierać warunki i termin płatności, przy czym termin płatności ma być nie krótszy niż 30 dni;

f) być złożona w formie elektronicznej jako skan lub być złożona w formie elektronicznej podpisana kwalifikowanym podpisem elektronicznym (wówczas niewymagana jest pieczęć firmowa).

2. Zawartość oferty w kolejności jak poniżej:
   - Załącznik nr 2 – Formularz ofertowy.
   - Załącznik nr 3 – Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu.
   - Załącznik nr 4 – Oświadczenie dotyczące powiązań osobowych lub kapitałowych.
   - Załącznik nr 5 – Formularz dotyczący warunków RODO.
   - Załącznik nr 6 – Oświadczenie o niezaleganiu z płatnościami na rzecz podmiotów publicznych i prywatnych.
   - Załącznik nr 7 – Wykaz zrealizowanych zamówień.
   - Załącznik nr 8 – Specyfikacja techniczna i karty katalogowe oferowanych towarów potwierdzające spełnienie wymagań opisanych w Załączniku nr 1 SWZ.
   - Załącznik nr 9 – Warunki gwarancji oferowanych towarów.

JSW IT Systems Sp. z o.o. jednocześnie informuje, że wybrany Wykonawca może być sprawdzany pod kątem:

a) Faktu istnienia i prowadzenia działalności oraz poprawności danych przekazanych przez Wykonawcę, z użyciem baz danych:
   - Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEiDG) https://prod.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx lub
   - Krajowego Rejestru Sądowego (KRS) https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/index.html oraz
   - Bazy REGON Głównego Urzędu Statystycznego (REGON – GUS): https://wyszukiwarkaregon.stat.gov.pl/appBIR/index.aspx
   - Bazy Krajowego Rejestru Długów Biura Informacji Gospodarczej SA (KRD): https://krd.pl/

b) Weryfikacji statusu podmiotu jako czynnego podatnika VAT, z użyciem baz danych:
   - Portalu Podatkowego Ministerstwa Finansów: https://ppuslugi.mf.gov.pl/_/#3 („Sprawdź podmiot w VAT”) oraz
   - Wykazu podmiotów niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT Ministerstwa Finansów: https://www.mf.gov.pl/krajowa-administracja-skarbowa/dzialalnosc/wykaz-podmiotow-niezarejestrowanych-oraz-wykreslonych-i-przywroconych-do-rejestru-vat lub
   - Bazy VIES Komisji Europejskiej – dla transakcji transgranicznych: http://ec.europa.eu/taxation_customs/vies/vatResponse.html

c) Weryfikacji na listach sankcyjnych pod względem przeciwdziałania wspieraniu agresji i ochrony bezpieczeństwa narodowego https://www.gov.pl/web/mswia/decyzje-ministra-swia-w-sprawie-wpisu-na-liste-sankcyjna

d) Weryfikacji innych dostępnych w domenie publicznej informacji na temat legalności działalności Wykonawcę z uwzględnieniem:
   - Strony Internetowej Kontrahenta;
   - Innych informacji i opinii dot. działalności prowadzonej przez Kontrahenta.

Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do uzupełnienia oferty o dokumenty potwierdzające spełnienie warunków udziału w postępowaniu, np.: sprawozdanie finansowe lub jego część, oświadczenie Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, potwierdzenie posiadania ubezpieczenia od odpowiedzialności cywilnej w zakresie prowadzonej działalności, związanej z przedmiotem zamówienia o wartości co najmniej równej wartości oferty netto, informacje banku lub spółdzielczej kasy oszczędnościowo kredytowej potwierdzająca wysokość posiadanych środków finansowych, lub zdolność kredytową Wykonawcy w okresie nie wcześniejszym niż 1 miesiąc przed upływem terminu składania ofert, referencje.
Złożenie oferty przez Wykonawcę jest równoznaczne z wyrażeniem zgody na podejmowanie ww. działań weryfikacyjnych przez Zamawiającego oraz przekazywania tak uzyskanych informacji na rzecz podmiotu dominującego tj. Jastrzębskiej Spółki Węglowej S.A. oraz podmiotów powiązanych.

3.2. Warunki udziału w postępowaniu.

1) Dysponowanie odpowiednim potencjałem technicznym oraz personelem zdolnym do wykonania przedmiotu zamówienia (wypełniony załącznik nr 3).
2) Zrealizowanie w okresie 3 ostatnich lat, co najmniej 2 zamówień odpowiadających przedmiotowi zamówienia odpowiednio dla urządzeń oferowanych w ramach danego Zadania (wypełniony załącznik nr 7), dostarczenie referencji lub innych dokumentów potwierdzających prawidłową realizację zamówienia.
3) Brak powiązania osobowego lub kapitałowego z Zamawiającym, gdzie przez powiązania osobowe lub kapitałowe rozumie się wzajemne powiązania pomiędzy Zamawiającym, osobą upoważnioną do zaciągania zobowiązań w imieniu Zamawiającego, osobami wykonującymi czynności związane z przygotowaniem i prowadzeniem procedury wyboru a Wykonawcą, polegające w szczególności na:
   - uczestniczeniu w spółce jako wspólnik spółki cywilnej lub osobowej;
   - posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez instytucję zarządzającą programem operacyjnym ;
   - pełnieniu funkcji członka organu nadzorczego, zarządczego, prokurenta pełnomocnika;
   - pozostawania w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

     Wykonawcy, którzy nie wykażą spełnienia ww. warunków określonych zostaną wykluczeni z prowadzonego postępowania. (wypełniony załącznik nr 6).
4) Sytuacja finansowa i ekonomiczna zapewniająca realizację przedmiotu zamówienia, przez co Zamawiający rozumie:
   a) Wykonawca posiada środki finansowe pozwalające na realizację całości zamówienia, potwierdzone informacją banku lub spółdzielczej kasy oszczędnościowo kredytowej, potwierdzającą wysokość posiadanych środków finansowych lub zdolność kredytową Wykonawcy, w okresie nie wcześniejszym niż 1 miesiąc przed upływem terminu składania ofert,

b) Wykonawca posiada ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia o wartości co najmniej równej wartości oferty netto.

5) Zamawiający wyklucza z postępowania Wykonawcę nie spełniającego warunków udziału w postępowaniu.

3.3. Okres ważności oferty.

Minimalny okres ważności oferty to 90 dni.

3.4. Postanowienia dotyczące Wykonawców wspólnie składających ofertę (konsorcja, spółki cywilne).

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia (konsorcjum, spółka cywilna). W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy.
2. Na formularzu oferty, jak również innych dokumentach powołujących się na „Wykonawca”, w miejscu „nazwa i adres Wykonawcy” należy wpisać dane dotyczące konsorcjum lub spółki cywilnej, a nie pełnomocnika, a do oferty należy załączyć pełnomocnictwo.
3. Przepisy dotyczące Wykonawcy stosuje się odpowiednio do Wykonawców wspólnie składających ofertę.
4. Każdy z warunków określonych w pkt 3.2. (warunki udziału w postępowaniu) winien spełniać co najmniej jeden z Wykonawców samodzielnie albo wszyscy Wykonawcy wspólnie.
5. Oświadczenie wymienione w Załączniku nr 3 i 4 składa każdy z Wykonawców wspólnie składających ofertę w celu potwierdzenia spełniania warunków udziału w postępowaniu oraz braku podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
6. Oświadczenie wymienione w Załączniku nr 6 każdy z Wykonawców wchodzących w skład konsorcjum lub wspólników spółki cywilnej składa samodzielnie.
7. Wykonawcy występujący wspólnie ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie umowy.
8. W przypadku, gdy oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia zostanie wybrana, Zamawiający może żądać przed zawarciem umowy określonej w niniejszym SWZ umowy regulującej współpracę tych Wykonawców.

3.5. Miejsce i termin składania ofert.

- Oferta powinna być złożona w formie elektronicznej lub w formie podpisanego przez osoby upoważnione skanu na adres:

przetargi@jswits.pl

do dnia 23.03.2023 r., godz. 12.00

w temacie należy podać:

„Postępowanie nr 07/2023”

- Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
- W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty.

3.6. Sposób komunikacji z Zamawiającym.

Pytania powinny być zgłaszane najpóźniej **do dnia 17.03.2023 r. godz. 12.00**, wyłącznie w formie elektronicznej za pośrednictwem Bazy Konkurencyjności w zakładce „Pytania” w ramach przedmiotowego postępowania.

Odpowiedzi zostaną zamieszczone w Bazie Konkurencyjności w zakładce „Pytania” w ramach przedmiotowego postępowania.

Zamawiający nie będzie udzielał odpowiedzi na pytania złożone w inny, niż opisano powyżej, sposób.

3.7. Opis kryteriów i sposobu oceny ofert.

Każde zadanie będzie odrębnie podlegać ocenie zgodnie z poniższymi kryteriami.

Tabela nr 1 Kryteria oceny ofert.

Lp.	Nazwa kryterium	Waga	Wzór
1	**Cena netto (C) przedmiotu zamówienia dla poszczególnego zadania**	**85**	**C = Cmin x waga / Co**, gdzie: **Cmin** – najniższa cena netto przedmiotu zamówienia dla poszczególnego zadania w ofertach złożonych w postępowaniu; **Co** – cena netto za realizację przedmiotu oferty ocenianej;
2	**Termin realizacji**	**15**	**15 pkt. gdy termin realizacji do 14 dni od daty zamówienia** **5 pkt. gdy termin realizacji do 30 dni od daty zamówienia** **0 pkt. gdy termin realizacji powyżej 30 dni od daty zamówienia ale nie więcej niż 90 dni.**

Zamawiający zastrzega możliwość odrzucenia oferty, która zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.
Każde z wymienionych powyżej kryteriów zostało oznaczone odpowiednią wagą, gdzie waga wyznacza istotność danego kryterium przy dokonywaniu oceny oferty.
Zamawiający dokona oceny ofert, każdego zadania odrębnie, w zakresie kryteriów, które przedstawiono w tabeli powyżej. Zamawiający dokona weryfikacji oraz przypisania punktów dla poszczególnych kryteriów oraz wyliczy **Łączną ocenę punktową** oferty dla każdego z zadań odrębnie (ident. O) według następującego wzoru:

O = C +T

3.8. Informacja o formalnościach po wyborze oferty.

Zamawiający poinformuje Wykonawcę, którego oferta została wybrana, o terminie i formie zawarcia Umowy.

4. Odrzucenie oferty.

Zamawiający zastrzega sobie prawo do odrzucenia oferty:

a) Złożonej po terminie do składania ofert wskazanym przez Zamawiającego,
b) Niekompletnej lub niespełniającej wymagań wskazanych w SWZ,
c) Niezgodnej z powszechnie obowiązującymi przepisami prawa,
d) Niespełniającej warunków udziału w postępowaniu,
e) Jeżeli jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji,
f) Zawierającej rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia,
g) Jeżeli Wykonawca nie wyraził zgody na przedłużenie terminu związania ofertą,
h) Jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, w tym bezpieczeństwo podmiotów objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122), a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób,
i) Została złożona przez wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia,
j) Jeżeli w stosunku do Wykonawcy zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 129).

5. Klauzula ochrony informacji

Wykonawca zobowiązuje się do traktowania wszelkich informacji wynikających z faktu otrzymania SWZ oraz odpowiedzi w niniejszym zamówieniu oraz prowadzonych rozmów handlowych za poufne. Ww. informacje mogą być udzielane przez Wykonawcę jedynie po uzyskaniu pisemnej zgody JSW IT Systems Spółka z o.o. na przekazanie takich informacji. W przypadku, jeżeli Wykonawca, który otrzymał SWZ nie zgadza się z powyższymi klauzulami, niniejszy materiał powinien natychmiast zwrócić do JSW IT Systems Spółka z o.o., a wszystkie kopie (elektroniczne jak i papierowe) zniszczyć.
Ponadto informujemy, że:

a) Administratorem Pani/Pana danych osobowych jest JSW IT Systems Spółka z o.o. z siedzibą w Jastrzębiu-Zdroju (44-330) przy ul. Armii Krajowej 56, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy X Wydział Gospodarczy KRS w Gliwicach, pod numerem KRS 0000083839.
b) Powołano Inspektora Ochrony Danych Osobowych, z którym może Pani/Pan skontaktować się: telefonując pod numer: 32 7002745 od poniedziałku do piątku w godz. 7.00 – 15.00, pisząc na adres

mailowy: *iod@jswits.pl* lub pocztą tradycyjną na adres siedziby JSW IT Systems Spółka z o.o.

c) Pani/Pana dane osobowe będą przetwarzane w celu:
   - Przeprowadzenia postępowania ofertowego;
   - Zapewnienia kontaktów biznesowych wyłącznie pomiędzy Pani/Pana firmą lub firmą, którą Pani/Pan reprezentuje a JSW IT Systems Spółka z o.o.

d) W przypadku wyboru oferty i zawarcia umowy Pani/Pana dane osobowe będą przetwarzane w następujących celach:
   - Zawarcia i prawidłowej realizacji umowy;
   - Podatkowych;
   - Tworzenia raportów na rzecz podmiotu dominującego;
   - Dla dochodzenia roszczeń wynikających z przepisów prawa cywilnego, jeśli takie się pojawią.

e) Podstawą prawną przetwarzania Pani/Pana danych osobowych jest wykonanie umowy, której jest Pani/Pan stroną lub do podjęcia działań na Pani/Pana żądanie przed zawarciem umowy (art. 6 ust. 1 lit. b ogólnego rozporządzenia ochrony danych) oraz na podstawie art. 6 ust. 1 lit. f) ogólnego rozporządzenia ochrony danych.

f) Podanie przez Pani/Pana danych osobowych jest dobrowolne, lecz konieczne do przeprowadzenia postępowania ofertowego i/lub zawarcia i wykonania umowy.

g) Ma Pani/Pan prawo do żądania od administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do przenoszenia. W przypadku danych przekazanych na podstawie art. 6 ust. 1 lit. f) ogólnego rozporządzenia ochrony danych przysługuje Pani/Panu prawo do wniesienia sprzeciwu wobec przetwarzanych danych.

h) Pani/Pana dane osobowe będą przechowywane przez cały czas trwania umowy oraz po jej ustaniu do czasu wypełnienia obowiązków wynikających z przepisów prawa oraz na potrzeby sprawozdawczości.

i) Odbiorcami Pani/Pana danych osobowych mogą być podmioty:
   - Świadczące na naszą rzecz usługi tj. przesyłki kurierskie i Poczta Polska;
   - Jastrzębska Spółka Węglowa S.A. i podmioty powiązane;
   - Doradcy prawni i podatkowi.

j) Pani/Pana dane osobowe nie będą przekazywane do państw trzecich/organizacji międzynarodowych.

k) Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany.

l) Jeżeli uzna Pani/Pan, że Pani/Pana dane osobowe będą przetwarzane niezgodnie z wymogami prawa, przysługuje Pani/Panu prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

5. Postanowienia końcowe.

a) Za opracowanie lub złożenie oferty nie przysługuje wynagrodzenie, oferta nie podlega zwrotowi.

b) Wykonawca z chwilą złożenia oferty zobowiązuje się do zachowania w poufności wszelkich informacji jakie pozyskał w toku postępowania ofertowego, w szczególności pozyskanych informacji technicznych, ekonomicznych i organizacyjnych dotyczących Zamawiającego.
c) W kwestiach nieuregulowanych zastosowanie mają odpowiednie przepisy Kodeksu Cywilnego.

6. Załączniki

- Załącznik nr 1 – Specyfikacja przedmiotu zamówienia dla poszczególnych zadań
- Załącznik nr 2 – Formularz ofertowy;
- Załącznik nr 3 – Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu.
- Załącznik nr 4 – Oświadczenie dotyczące powiązań osobowych lub kapitałowych.
- Załącznik nr 5 – Formularz dotyczący warunków RODO.
- Załącznik nr 6 – Oświadczenie o niezaleganiu z płatnościami na rzecz podmiotów publicznych i prywatnych.
- Załącznik nr 7 – Wykaz zrealizowanych zamówień.
- Załącznik nr 8 – Istotne postanowienia umowne.

Załącznik nr 1 do SWZ

Specyfikacja Przedmiotu Zamówienia

1. Zadanie nr 1.

Przełącznik sieci LAN montowany do szafy RACK 19” – 1 szt.

Rodzaj urządzenia:

1. Przełącznik typu standalone wyposażony w 24 porty 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty 40/100 Gigabit Ethernet QSFP.
2. Porty SFP/SFP+/SFP28 powinny umożliwiać zastosowanie następujących wkładek interfejsowych:
   - Gigabit Ethernet 1000Base-T,
   - Gigabit Ethernet 1000Base-SX,
   - Gigabit Ethernet 1000Base-LX/LH,
   - Gigabit Ethernet 1000Base-EX,
   - Gigabit Ethernet 1000Base-ZX,
   - Gigabit Ethernet 1000Base-BX-D/U,
   - 10Gigabit Ethernet 10GBase-SR,
   - 10Gigabit Ethernet 10GBase-LR,
   - 10Gigabit Ethernet 10GBase-ER,
   - 10Gigabit Ethernet 10GBase-ZR,
   - 10Gigabit Ethernet 10GBase-BX-D/U,
   - 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
   - 25Gigabit Ethernet 25GBASE-SR,
   - 25Gigabit Ethernet typu twinax (SFP28 – SFP28),
   - 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
   - 10/25Gigabit Ethernet 10/25GBASE-LR (SMF).
3. Porty QSFP powinny umożliwiać zastosowanie następujących modułów interfejsowych:
   Dla transmisji 40Gb/s:
   - 40G-SR4,
   - 40G-LR4,
   - 40G-ER4,
   - 40G-SR-BD,
   - 40G-CSR,
   - 40G-CSR4,
   - 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),
   - adapter 40G QSFP->10G SFP+,
   - 40Gigabit Ethernet typu twinax (QSFP - QSFP);

   Dla transmisji 100Gb/s:
   - 100GBASE-SR4,
   - 100GBASE-LR4,
   - 100Gigabit Ethernet typu twinax (QSFP - QSFP).

Architektura:

1. Urządzenie powinno być wyposażone w wymienne moduły wentylatorów.
2. Urządzenie powinno mieć możliwość wyposażenia w zasilacz redundantny do pracy w trybie 1:1.

3. Urządzenie powinno być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem. Urządzenia w klastrze powinny zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3.
4. Klastrowanie powinno wspierać funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami.

Oczekiwana wydajność:

1. Minimum 16GB pamięci DRAM i 16GB pamięci flash.
2. Urządzenie powinno posiadać 32MB bufor pamięci.
3. Przepustowość przełącznika (switching capacity) minimum 1.6 Tbps.
4. Prędkość przesyłania (forwarding rate) minimum 1 miliard pps (1Bpps).
5. Obsługa minimum:
    - 1000 aktywnych sieci VLAN,
    - 80000 adresów MAC,
    - 212000 tras IPv4,
    - 212000 tras IPv6,
    - 27000 wpisów w listach kontroli dostępu Security ACL,
    - 16000 wpisów w listach kontroli dostępu QoS ACL,
    - 1000 interfejsów SVI L3,
    - Jumbo frame o rozmiarze 9198 B,
    - 128 połączeń zagregowanych, tzw. port-channel,
    - 16 linków w ramach jednego połączenia zagregowanego LACP.

Oprogramowanie/funkcjonalność:

1. Obsługa protokołu NTP.
2. Obsługa IGMPv1/2/3.
3. Obsługa standardu IEEE 802.1ae (MACSec), szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Przełącznik powinien wspierać uruchomienie MACsec na portach tworzących połączenia zaagregowane L2 i L3.
4. System operacyjny przełącznika powinien umożliwiać wgrywanie poprawek bez konieczności restartowania platformy.
5. System operacyjny przełącznika powinien mieć możliwość konfiguracji poprzez API za pomocą m.in. protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwiać eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
6. Wsparcie dla protokołu RESTCONF.
7. Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia.
8. Przełącznik powinien realizować następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    - IEEE 802.1w Rapid Spanning Tree,
    - IEEE 802.1s Multi-Instance Spanning Tree,
    - Obsługa minimum 1000 instancji protokołu STP.
9. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED.
10. Możliwość realizacji funkcji 802.1Q tunneling (QinQ).
11. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
12. Obsługa 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik powinien umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level).
13. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+.
14. Obsługa list kontroli dostępu (ACL) następujących typów:

- Port ACL umożliwiających kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
- VLAN ACL umożliwiających kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
- Routed ACL umożliwiających kontrolę ruchu routowanego pomiędzy sieciami VLAN.

15. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia).
16. Przełącznik powinien realizować następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    - 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    - Implementację algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    - Kontrola sztormów dla ruchu broadcast/multicast/unicast,
    - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
17. Przełącznik powinien posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing).
18. Realizacja funkcji Private VLAN na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk).
19. Urządzenie powinno realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
    - Routing statyczny dla IPv4 i IPv6,
    - Routing dynamiczny dla IPv4: BGP, ISIS,
    - Routing dynamiczny dla IPv4: OSPF,
    - Routing dynamiczny dla IPv6: OSPFv3,
    - Funkcjonalności Policy-based routing,
    - multicast routing (PIM-SM, PIM-SSM),
    - Obsługa protokołu redundancji bramy,
    - Obsługa minimum 200 tuneli GRE (Generic Routing Encapsulation),
    - Obsługa minimum 1000 wirtualnych instancji routingu,
20. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa minimum 100 sesji BFD.
21. Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji.
22. Realizacja protokołu LISP zgodnie z RFC 6830.
23. Możliwość enkapsulacji ruchu przy pomocy VXLAN.
24. Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border.
25. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
26. Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego.
27. Funkcjonalność sondy do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla: DHCP, DNS, FTP, HTTP, ICMP,-TCP, UDP.
28. Funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego.

29. Wbudowany analizator pakietów.
30. Możliwość uruchamiania dodatkowych aplikacji w kontenerach Docker.
31. Możliwość wyposażenia urządzenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności 240/480/960 GB.
32. Możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych.
33. Możliwość modyfikacji programowej takich parametrów urządzenia jak:
    - Ilość pozycji w tablicy MAC,
    - Ilość tras routingowych unicast i multicast,
    - Ilość tras w sieci MPLS VPN,
    - Ilość obsługiwanych sesji netflow.
34. Realizacja następujących funkcjonalności z zakresu MPLS:
    - L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC,
    - L2VPN - Virtual Private LAN Services (VPLS) - obsługa do 1000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
    - L3 VPN - MPLS Virtual Private Network (VPN),
    - Multicast VPN (MVPN),
    - Inter AS Option A i B,
    - EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
    - MPLS over GRE.

Zarządzanie i konfiguracja:

1. Urządzenie powinno realizować sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni minimum 98000.
2. Dedykowany port Ethernet do zarządzania out-of-band.
3. Urządzenie powinno być wyposażone w port konsoli USB.
4. Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność powinna umożliwiać kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA.
5. Urządzenie powinno posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie powinno wspierać możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.
6. Możliwość tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
7. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
8. Urządzenie powinno posiadać wbudowany tag RFID w celu łatwej identyfikacji.
9. Urządzenie powinno wspierać funkcję programowego resetu do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące.

Obudowa:

1. Możliwość montażu w szafie rack 19”.
2. Wysokość urządzenia 1 RU.
3. Głębokość chassis urządzenia z wentylatorami i zasilaczami – mniejsza niż 50 cm.

Wyposażenie:

Przełącznik powinien być wyposażony w:

1. zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy.
2. licencję subskrypcyjną na wymagane funkcjonalności na okres min. 3 lat.

3. dwa moduły interfejsowe QSFP 40G-LR4.

Gwarancja:
Warunki gwarancji nie gorsze niż warunki gwarancji producenta sprzętu.
Okres gwarancji minimum 3 lata.

2. Zadanie nr 2.

Przełącznik sieci LAN montowany do szafy RACK 19” – 2 szt.

Rodzaj urządzenia:

1. Przełącznik L3
2. Porty przełącznika: 8x 10/100/1000Base-T oraz 24 x 1000/10GBase-X (SFP+) oraz 2 x 40GBase-X (QSFP)
3. Port konsolowy: RJ45 (RS-232)
4. Bufor pakietów: minimum 4MB
5. Ramki Jumbo: minimum 16K
6. Tablica adresów MAC: minimum 32K
7. Tablica VLAN: minimum 1K
8. Pamięć Flash: minimum 32MB
9. Pamięć RAM: minimum 512MB
10. IEEE 802.1D STP/802.1w RSTP/802.1s MSTP
11. IEEE 802.3ad LACP
12. Virtual Cable Testing
13. VRRP
14. Loop guard
15. 802.1Q VLANs
16. LACP algorithm of source/destination IP (load balance)

Bezpieczeństwo:

17. Filtrowanie w warstwie 2
18. BPDU Tunne
19. BPDU Guard
20. Uwierzytelnienie i autoryzacja logowania poprzez RADIUS oraz TACACS+
21. SSH v1/v2
22. DHCP/DHCPv6 snooping
23. Port security
24. IEEE 802.1x port-based / mac-based

Routing:

25. Routing statyczny IPv4 / IPv6
26. RIP v1,v2 / RIPng
27. OSPF v2 / OSPF v3
28. BGP / BGP4+

Zarządzanie:

29. GUI (Web)
30. SNMP v1/v2c/v3
31. Configuration backup and restore

32. Wielopoziomowy CLI
33. sFlow
34. Port Mirroring per IP/TCP/UDP
35. Cluster
36. Stack (VSF)
37. Stack (VSF-HA)
38. Wszystkie dostępne funkcjonalności bez konieczności zakupu dodatkowych licencji

Zasilanie:

39. Zasilanie podstawowe – 230V AC
40. Zasilanie redundantne – 48V DC

Wymiary:

41. Montaż w szafie teleinformatycznej rack 19”
42. Wysokość: 1U
43. Głębokość – max 350 mm

Gwarancja:
Warunki gwarancji nie gorsze niż warunki gwarancji producenta sprzętu.
Okres gwarancji minimum 3 lata

3. Zadanie nr 3.

Przełącznik sieci LAN montowany na szynę DIN TH35mm, – 1 szt.

Rodzaj urządzenia:

1. Przełącznik sieci Ethernet wyposażony w 8 portów Fast Ethernet SFP oraz 4 porty Gigabit Ethernet typu combo (SFP/RJ45).
2. Przełącznik powinien być przystosowany do pracy w warunkach przemysłowych (wsparcie dla norm przemysłowych: EN 61000-6-1, EN 61000-6-2, EN 61000-6-4, EN 61326, EN 61131-2, IEEE 1613, IEC 61850-3).
3. Urządzenie powinno posiadać certyfikaty bezpieczeństwa - UL/CSA 60950-1, EN 60950-1.
4. Porty Fast Ethernet SFP powinny umożliwiać zastosowanie następujących wkładek interfejsowych:
    - 100FX,
    - 100LX,
    - 100EX,
    - 100ZX,
    - 100BX.
5. Porty Gigabit Ethernet SFP powinny umożliwiać zastosowanie następujących wkładek interfejsowych:
    - SX,
    - LX,
    - ZX,
    - CWDM,
    - DWDM,
    - BX.

Architektura:

1. Urządzenie powinno spełniać następujące kryteria dotyczące zasilania:

- zasilanie prądem stałym, z możliwością dołączenia redundantnych źródeł zasilania z napięciem wejściowym w zakresie 9 – 60 VDC,
- pobór mocy do 42W.

2. Urządzenie powinno posiadać co najmniej dwa wejścia I/O służące do podłączania źródeł alarmowych oraz co najmniej jedno wyjście alarmowe.
3. Zakres temperatury pracy przełącznika powinien zawierać się w przedziałach:
   - od -40 do +75 st. C w mechanicznie wentylowanej szafce,
   - od -40 do +60 st. C w szafce bez wentylacji.
4. Możliwa wilgotność środowiska pracy (bez kondensacji) powinna mieścić się w zakresie 5 – 95%.
5. Deklarowany średni czas bezawaryjnej pracy MTBF – co najmniej 580000 godzin.
6. Przełącznik powinien być wyposażony w wymienną kartę pamięci flash SD do przechowywania plików z oprogramowaniem i konfiguracją; z możliwością wymiany przełącznika bez jego rekonfiguracji (poprzez wymianę karty pamięci).
7. Urządzenie powinno spełniać następujące normy środowiskowe: IEC 60068-2-27 (operational shock, 50G, 11ms, Half Sine), IEC 60068-2-27 (Non-Operational Shock, 65-80G, 9ms, Trapezoidal), IEC 60068-2-6, IEC 60068-2-64, EN 61373 (Operational Vibration), IEC 60068-2-6, IEC 60068-2-64, EN 61373 (Non-operational Vibration), ISO 9223: Corrosion, class C3-Medium, class C4-High, EN 60068-2-52 (Salt Fog), EN 60068-2-60 (Flowing Mixed Gas).

Oczekiwana wydajność:

1. Co najmniej 1 GB pamięci DRAM oraz 128MB pamięci flash, karta SD minimum 1GB.
2. Wydajność zapewniająca możliwość pracy z pełną szybkością wszystkich portów (tzw. line rate) dla ramek 64 bajtów.
3. Tablica adresów MAC – co najmniej 16000 wpisów.
4. Obsługa minimum 1000 sieci VLAN 802.1Q.

Oprogramowanie/funkcjonalność:

1. Obsługa co najmniej 128 instancji dla protokołu STP.
2. Przełącznik powinien wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   - Możliwość klasyfikacji ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, ethertype,
   - Implementacja minimum czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi,
   - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu dla poszczególnych klas obsługi.
3. Przełącznik powinien posiadać funkcjonalność serwera DHCP oraz agenta DHCP relay.
4. Przełącznik powinien posiadać możliwość skonfigurowania translacji adresów IP w oparciu o L2 Network Address Translation.
5. Obsługa ruchu multicast realizowana z wykorzystaniem IGMPv1, v2 i v3, filtrowanie IGMP.
6. Wsparcie dla protokołów L2 oraz mechanizmów niezawodności:
   - Wykrywanie łącz jednokierunkowych,
   - Agregacja portów zgodnie ze standardem 802.3ad,
   - Obsługa ruchu w topologiach pierścieniowych,
   - Obsługa Spanning Tree: 802.1w RSTP, 802.1s MSTP,
   - Obsługa protokołu Parallel Redundancy Protocol,
   - Obsługa protokołu High-availability Seamless Redundancy,
   - Obsługa protokołu Media Redundancy Protocol wraz z możliwością konfiguracji urządzenia jako Client, Manager, Auto Manager,
   - Możliwość konfiguracji kombinacji protokołów w przylegających pierścieniach:

HSR-HSR Quadbox, HSR-PRP Dual RedBox,

7. Możliwość definiowania poziomów dostępu administracyjnego poprzez konsolę.
8. Autoryzacja urządzeń końcowych w oparciu o IEEE 802.1x, z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL.
9. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
10. Obsługa funkcji Guest VLAN.
11. Obsługa list kontroli dostępu (ACL).
12. Obsługa mechanizmów DHCP Snooping, Dynamic ARP Inspection, IP Source Guard.
13. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
14. Wsparcie dla protokołów industrialnych: CIP EtherNet/IP, PROFINET, IEEE 1588 PTP v2, Modbus TCP/IP, GOOSE.
15. Wsparcie dla mechanizmów kontroli usług ethernetowych Ethernet OAM, IEEE 802.3ah, CFM - IEEE 802.1ag.
16. Możliwość uruchomienie mechanizmów L3:
    - Routing statyczny i dynamiczny dla IPv4 (RIPv2, OSPF, IS-IS, BGPv4) oraz IPv6 (RIPng, OSPFv3),
    - Multicast routing (PIM-SM, PIM-DM, PIM sparse-dense mode),
    - Policy-based routing.
17. Możliwość szyfrowania zgodnie z IEEE 802.1AE MACSec.

Zarządzanie i konfiguracja:

1. Możliwość oprogramowania lub oskryptowania własnych funkcjonalności, niedostępnych natywnie w dostarczanym oprogramowaniu. Możliwość wprowadzenia kodu programu lub skryptu bezpośrednio na urządzenie, bez udziału producenta oraz uruchamianie lokalnie na urządzeniu.
2. Wsparcie dla protokołów SSHv2, SNMPv3.
3. Autoryzacja prób logowania do urządzenia za pomocą serwerów RADIUS lub TACACS+.
4. Możliwość zarządzania urządzeniem poprzez interfejs graficzny
5. Dostęp poprzez port konsoli (RS-232 oraz mini-USB)
6. Plik konfiguracyjny urządzenia powinien być plikiem tekstowym, z możliwością edycji w trybie off-line.
7. Możliwość dostępu do wybranych parametrów urządzenia poprzez protokół Modbus.
8. Możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu – zarówno lokalnie, jak i zdalnie.

Obudowa:

3. Obudowa urządzenia powinna być zgodna ze stopniem ochrony co najmniej IP30.
4. Montaż urządzenia – na szynie DIN.

Wyposażenie:

Przełącznik powinien być wyposażony w:

1. licencję subskrypcyjną na wymagane funkcjonalności na okres min. 3 lat.

Gwarancja:

Warunki gwarancji nie gorsze niż warunki gwarancji producenta sprzętu.
Okres gwarancji minimum 3 lata.

4. Zadanie nr 4.

Przełącznik sieci LAN montowany na szynę DIN TH35mm – 4 szt.

Rodzaj urządzenia:

1. Porty przełącznika: minimum 8x 10/100/1000Base-T RJ45 oraz minimum12x 100/1000Base-X SFP
2. Port konsolowy: RJ45 (RS-232)
3. Bufor pakietów: minimum 0,5MB
4. Ramki Jumbo: minimum 9,6k
5. Tablica adresów MAC: minimum 8k
6. Tablica VLAN: minimum 4094
7. Pamięć Flash: minimum 16MB
8. Pamięć RAM: minimum 128MB
9. Algorytm pracy: Store and Forward
10. Chłodzenie: pasywne
11. Temperatura pracy: zakres minimum -40°C - 75°C
12. Zasilanie: redundantne DualDC 12/24/48V/-48 (9,6-60VDC).
13. Zabezpieczenie przeciwprzepięciowe: minimum 4kV
14. Zużycie energii: maximum 15.8W
15. Terminal block: dwa niezależne zasilania + styk alarmu, 6 Pin
16. Wymiary: maksymalna: szerokość 106 mm, wysokość 72mm, głębokość 52mm
17. Waga: mniejsza lub równa 1 kg
18. Montaż: szyna DIN

Certyfikaty Bezpieczeństwa:

1. EMC: CE (EN55032, EN55035), RoHS
2. EMI: FCC Part 15 Subpart B Class A.CE EN 55022 Class A
3. EMS: EN61000-4-2 (ESD); -3 (RS); -4 (BURST); -5 (Surge); - 6 (CS); -8 (PFMF, Magnetic Field)
4. Safety: EN62368-1
5. Shock: IEC 60068-2-27
6. Freefall: IEC 60068-2-32
7. Vibration: IEC 60068-2-6

Oprogramowanie/funkcjonalność:

1. Obsługa VLAN: Voice VLAN, IP Subnet based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, GVRP, MVR, IEEE 802.1Q, Normal QinQ, Selective QinQ, Flexible QinQ
2. DHCP: DHCP Client, DHCP Relay, Option 82, DHCP Snooping, DHCP Server
3. Drzewo rozpinające: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP
4. Multi Ringi: do 5 instancji, z których każda obsługuje µ-Ring, µ-Chain lub Sub-Ring do elastycznych zastosowań i maksymalnie 5 pierścieni. Czas regeneracji <10ms. Maksymalna dozwolona liczba urządzeń w pierścieniu obsługiwanym przez Ring to 250.
5. Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms, Loopback Detection, ITU-T G.8031 /Y.1342 EPS
6. Agregacja linków: Static (Hash witch SA, DA, IP, TCP/UDP port dla 5 trunk grup. Dynamic IEEE 802.3ad (LACP), 5 groups per device
7. Bezpieczeństwo: Storm Control or Unicast, Broadcast, Multicast, Port Security, MAC Limit based on VLAN and Port,
8. Multicast: IGMP v1/v2/v3 snooping, IGMP Fast leave, Port Filtering Profile, MLD v1/v2 Snooping, Throttling, IGMP authentication, Query/Static Router, Group
9. QoS: IEEE 802.1p 8 active priorities queues for per port

10. Traffic Classification QoS: IEEE 802.1p based CoS, IP Precedence based CoS, IP DSCP based CoS
11. Traffic Classification QoS: QCL(QoS Control List): Frame Type, Source/Destination MAC, VLAN ID, PCP, DEI, QCE(QoS Control Entry): Protocol, Source IP, IP Fragment, DSCP, TCP/UDP port number
12. Lista Kontroli Dostępu: IP ACL, MAC ACL, TCP/UDP ACL, Port-Based, MAC-Based (IEEE 802.1X)
13. Diagnostyka: VCT, DDM, Ping, Trace Route, RSPAN
14. Uwierzytelnianie: RADIUS authentication & accounting; TACACS+ authentication & accounting, TACACS+ 3.0; HTTPS, HTTP; SSL / SSH v2; User NamePassword Authentication: Local Authentication, Remote Authentication (via RADIUS / TACACS+)
15. Zarządzanie: CLI; Web Based Management; Telnet; SNMP V1, V2c, V3; sFlow ; Modbus/TCP;
16. SW & Configuration Upgrade TFTP, HTTP; FTP client Supports for upload/download configuration; RMON I (1, 2, 3, 9 group), RMON II; MIB RFC1213, Private MIB; UPnP; BOOTP;; RARP; IP Source Guard; Port Mirroring; Event Syslog Syslog server (RFC3164); Warning Message: System syslog, e-mail, alarm relay; DNS Client, Proxy; IEEE 1588 PTP V2 Support 5 operating mode in each port, Ordinary-Boundary, Peer to Peer Transparent Clock,
17. End to End Transparent Clock, Master, Slave; NTP, SNTP Client; LLDP (IEEE 802.1ab) Link Layer Discovery Protocol LLDP-MED.
18. System NMS: Tak
19. Oszczędność energii: IEEE 802.3az (Energy Efficient Ethernet), zarządzanie optymalizacją zużycia energii, zarządzanie energią LED (intensywność świśnięcia),
20. Diagnostyka Kabli: Pomiar kabla UTP podczas pracy normalnej oraz odległość uszkodzenia kabla
21. Oprogramowanie oraz wsparcie techniczne: oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
22. MTBF: minimum 517,000 Godzin (MIL-HDBK-217)

Gwarancja:
Warunki gwarancji nie gorsze niż warunki gwarancji producenta sprzętu.
Okres gwarancji minimum 5 lat.

5. Zadanie nr 5

Zapora sieciowa nowej generacji (NGFW), montowana do szafy RACK 19” – 1 szt.

Rodzaj urządzenia:

1. Specjalizowane urządzenie sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
2. Całość sprzętu i oprogramowania jest dostarczana i wspierana przez jednego producenta. Producent oferowanego rozwiązania jest obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders od co najmniej 5 lat.
3. Urządzenie umożliwia działanie w następujących trybach pracy:
    a. routera (tzn. w warstwie 3 modelu OSI),
    b. mostu (tzn. w warstwie 2 modelu OSI),
    c. w trybie transparentnym (urządzenie nie posiada skonfigurowanych adresów IP na interfejsach sieciowych i pracuje w trybie przezroczystego łączenia interfejsów w pary),
    d. w trybie pasywnego nasłuchu (sniffer/tap).
4. System umożliwia pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. Urządzenie jest wyposażone w port konsoli szeregowej RJ45 oraz dedykowany port zarządzający 10/100/1000 Mbps.
6. Nie występują ograniczenia licencyjne dotyczące liczby chronionych komputerów w sieci wewnętrznej.
7. Urządzenie firewall posiada separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.

8. Urządzenie firewall posiada dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
9. Urządzenie firewall wspiera 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 obsługuje 4000 znaczników VLAN.
10. Urządzenie firewall wspiera protokół LACP.
11. Urządzenie firewall zgodnie z ustaloną polityką prowadzi kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
12. Urządzenie firewall działa zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Blokuje wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
13. Polityka zabezpieczeń firewall uwzględnia
    a. adresy IP źródłowe i docelowe,
    b. protokoły i usługi sieciowe,
    c. aplikacje,
    d. kategorie URL,
    e. użytkowników aplikacji i grupy,
    f. reakcje zabezpieczeń,
    g. logowanie zdarzeń (początek i koniec sesji),
    h. strefa wejściowa i wyjściowa.
14. Urządzenie firewall automatycznie identyfikuje aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji odbywa się co najmniej poprzez sygnatury. Urządzenie wykrywa co najmniej 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Pozwala na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
15. Identyfikacja aplikacji nie wymaga 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.
16. Urządzenie firewall pozwala na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku odbywa się na podstawie zawartości i metadanych pliku.
17. Ochrona przed atakami typu „Drive-by-download” zapewniana jest poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.
18. Urządzenie firewall jest zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI.
19. Urządzenie firewall wyposażone jest w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
20. Dostęp do urządzenia i zarządzania z sieci jest zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń pozwala na zdefiniowanie wielu administratorów o różnych uprawnieniach.
21. Urządzenie firewall umożliwia uwierzytelnianie administratorów wykorzystując: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH wspierane jest uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
22. Urządzenie firewall zapewnia możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integracji w tym zakresie z systemami:
    a. Active Directory,
    b. Terminal Services.
23. Polityka kontroli dostępu (urządzeń firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i utrzymywana jest nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości odbywa się również transparentnie.

24. Urządzenie firewall pozwala na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane zawierają informacje o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
25. Urządzenie firewall umożliwia tworzenie raportów dostosowanych do wymagań użytkownika, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów jest dostępny w formatach PDF, CSV i XML. Na urządzeniu dostępne jest także tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
26. Urządzenie firewall umożliwia tworzenie dynamicznych grup użytkowników. Przynależność do grupy bazuje na etykietach a proces oznaczania etykiet pozwala na użycie:
    a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia),
    b. API.
27. Urządzenie firewall posiada funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP pozawalają na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
28. Urządzenie firewall obsługuje protokoły routingu dynamicznego, w tym: BGP, RIP, OSPF dla IPv4 i IPv6.
29. Urządzenie firewall obsługuje statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT umożliwiają dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
30. Urządzenie firewall posiada osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
31. Wykonywanie operacji translacji adresów NAT odnotowywane jest w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
32. Urządzenie firewall pozwala na selektywne wysyłanie logów do zewnętrznych systemów (np. Syslog) w zależności od ich rodzaju.
33. Urządzenie firewall obsługuje możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
34. Urządzenie firewall posiada możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
35. Wykonywanie operacji deszyfrowanie ruchu jest odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Zawiera informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Istnieje mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
36. Wykonywanie operacji deszyfrowania ruchu umożliwia wykorzystanie mechanizmów filtrowania URL.
37. Rozwiązanie umożliwia wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie: kategoryzacji stron URL oraz dodania własnych wyjątków.
38. Urządzenie zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
39. Dla deszyfrowania ruchu TLS 1.3 urządzenie zapewnia wsparcie dla X25519, X448 a także dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
40. Urządzenie firewall posiada funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
41. Umożliwia zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenie umożliwia stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
42. Firewall posiada możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
43. Posiada funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.

44. Posiada możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X- orwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesję w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
45. Urządzenie firewall umożliwia zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN oddbywa się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
46. Dla IKE zapewnione jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
47. Dla IPsec zapewnione jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
48. Urządzenie firewall zapewnia inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
49. Urządzenie firewall obsługuje funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta realizowana jest na bazie technologii SSL VPN oraz IPSec.
50. Funkcjonalność zdalnego dostępu VPN integruje się z funkcją rozpoznawania użytkowników.

Oczekiwana wydajność:

1. Firewall throughput http - min 5 Gbps
2. Firewall throughput appmix - min 4 Gbps
3. Threat Prevention throughput http - min 2 Gbps
4. Threat Prevention throughput appmix - min 2 Gbps
5. IPsec VPN throughput - min 3 Gbps
6. Max sessions - min 400 000
7. New sessions per second - min 70 000
8. 8 x 1000Base-T (input/output)

Oprogramowanie/funkcjonalności:

- **Threat Prevention**

1. Urządzenie firewall posiada funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS jest przechowywana na urządzeniu, jest regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co producent systemu zabezpieczeń.
2. Bezpośrednio w GUI urządzenia istnieje możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
3. Urządzenie firewall posiada funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
4. Urządzenie firewall posiada funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus przechowywana jest na urządzeniu, jest regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzi od tego samego producenta co firewall.
5. Urządzenie firewall posiada funkcję anty-spyware. Baza sygnatur jest przechowywania na urządzeniu, jest regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co system firewall.
6. Urządzenie firewall posiada funkcję ochrony DNS. Baza sygnatur jest przechowywania na urządzeniu, jest regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co system firewall.

- **Zaawansowana ochrona przed zagrożeniami**

1. Urządzenie posiada funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.

2. Rozwiązanie posiada możliwość analizy, identyfikacji oraz blokowania wcześniej nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w chmurze producenta, przy czym:
    a. wymagana analiza i detekcja umożliwia blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
    b. analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 jest możliwe dla ruchu typu: http, http2, ssl oraz niezidentyfikowanych przez firewall aplikacji w oparciu o TCP i UDP.

- **Zaawansowane filtrownie URL**

1. Kategoryzacja URL jest realizowana w oparciu o:
    a. Bazę kategorii utrzymywaną i aktualizowaną przez producenta składającą się z co najmniej 70 kategorii)
    b. Lokalny mechanizm kategoryzacji stron działający na bazie nauczania maszynowego (Machine Learning - ML)
    c. Zdalny mechanizm kategoryzacji stron działający na bazie nauczania maszynowego (Machine Learning - ML)
2. Wyżej wymienione opcje kategoryzacyjne oparte o nauczanie maszynowe (Machine Learning -ML) wykrywają i zapewniają ochronę przed złośliwymi stronami / atakami Phishing, złośliwymi skryptami JavaScript.

- **DNS Security**

Urządzenie firewall realizuje ochronę DNS w zakresie:

a. wykrywania zapytań do domen złośliwych (baza domen posiada nie mnie niż 10 milionów wpisów),
b. w przypadku wykrycia ruchu do nieznanej domeny firewall odpytuje serwer producenta o jej reputację
c. możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing),
d. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA),
e. wykrywanie domen dynamicznych Dynamic DNS,
f. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych,
g. wykrywanie domen śledzących (Trackery),
h. wykrywanie domen C&C,
i. wykrywanie domen hostowanych na dynamicznie przydzielanych adresach IP,
j. wykrywanie domen nowo zarejestrowanych (nie starszych niż 32 dni),
k. wykrywanie domen służących do przeprowadzania ataków phishing,
l. wykrywanie domen zaparkowanych,
m. wykrywanie domen służących do anonimizacji.

- **Oprogramowanie VPN dla stacji klienckiej**

1. Oprogramowanie klienta VPN dostępne dla Windows, MacOS, Linux, Android i iOS.
2. Urządzenie pozwala na zestawienie tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN
3. Oprogramowanie klienta VPN dla Windows i macOS posiada możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej w zakresie sprawdzenia:
    a. czy zainstalowano oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury,
    b. czy włączony jest osobisty firewall,
    c. czy włączone jest szyfrowanie dysku.
4. Usługa zdalnego dostępu oferuje elastyczne sposoby umieszczania / wykluczania ruchu w tunelu w oparciu o:

a. Adresacje docelową
b. Domeny docelowe
c. procesy źródłowe nawiązujące połączenia

5. Usługa zdalnego dostępu zapewnia możliwość zarówno umieszczenia jak i wykluczenia ruchu video z tunelu dla poniższych aplikacji:
   a. Dailymotion
   b. Hulu
   c. Netflix
   d. Sling
   e. Vimeo
   f. Xfinity
   g. Youku
   h. Youtube

- **SD-WAN**

1. Urządzenie umożliwia uruchomienie funkcjonalności SD-WAN. Firewall weryfikuje stan łącz w czasie rzeczywistym i w sposób dynamiczny wybierać optymalne łącze. Możliwe algorytmy wyboru łącza to: najlepsza dostępna, w kolejności od pierwszej do ostatniej, wagowa
2. W zakresie SD-WAN urządzenie zapewnia obsługę mechanizmu SLA (monitorowanie opóźnienia, zmienności opóźnienia, procentowej wartości traconych pakietów).
3. Monitoring parametrów SLA odbywa się nie tylko poprzez weryfikację drugiej strony tunelu IPSec VPN, ale także w oparciu o określony adres IP, FQDN
4. Urządzenie firewall posiada osobny zestaw polityk definiujący reguły SD-WAN rozdzielny od polityk bezpieczeństwa.
5. Dla aplikacji wrażliwych na parametry jakościowe istnieje możliwość przesyłania zduplikowanych pakietów (packet duplication), naprawy utraconych pakietów poprzez dodanie bitów parzystości przez stronę nadającą (Forward Error Correction)

- **Dodatkowe funkcjonalności**

1. Możliwość tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
2. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
3. Urządzenie powinno posiadać wbudowany tag RFID w celu łatwej identyfikacji.
4. Urządzenie powinno wspierać funkcję programowego resetu do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące.

Gwarancja:
Warunki gwarancji nie gorsze niż warunki gwarancji producenta sprzętu.
Okres gwarancji minimum 2 lata.

6. Zadanie nr 6

Urządzenie do podstawowych pomiarów i weryfikacji światłowodowych sieci optycznych

Wymagania podstawowe :

Urządzenie pomiarowe musi umożliwiać pomiar aktywnej sieci optycznej w wykonaniu jednomodowym (9/125um), wykorzystując falę o długości 1650 nm w zakresie identyfikacji uszkodzeń z analizą blokową. Urządzenie powinno pozwalać na pomiar jednomodowych (SM FO) sieci optycznych w zakresie odległości do 40 km. Ponadto, ten sam port optyczny urządzenia pomiarowego musi posiadać funkcjonalność miernika mocy optycznej dla wszystkich używanych okien transmisyjnych oraz zapewnić źródło światła 1650 nm do pomiarów tłumienia, z możliwością modulacji nadawanego sygnału.

Minimalne wymagania urządzenia pomiarowego :

Urządzenie musi umożliwiać pomiar długości trasy optycznej wraz z podaniem jej tłumienia oraz całkowitych strat odbiciowych w czasie nie dłuższym niż 3 sekundy, wraz z jej oceną jakościową, dla odległości do co najmniej 40 km.

Urządzenie musi posiadać tryb pomiarowy wskazujący jedynie niepoprawne zdarzenia na torze optycznym, które wymagają ingerencji instalatora. Wskazanie powinno uwzględnić pozycję w ciągu długości linii optycznej oraz parametry zdarzenia/zdarzeń. Tryb pomiarowy powinien pomijać poprawne zdarzenia, które nie wymagają dodatkowej ingerencji. Identyfikacja niepoprawnych zdarzeń może odbywać się w sposób automatyczny, lub za pomocą ustawionych przez użytkownika wartości progowych.

Pozostałe parametry i wymagane funkcjonalności:

- Filtr górnoprzepustowy z izolacją minimum 50dB, w zakresie od 1265 nm do 1617 nm.
- Wbudowane źródło światła o mocy wyjściowej > –8 dBm
- Wbudowany miernik mocy z zakresem pomiarowym od -60dBm do +15 dBm
- Urządzenie powinno być wyposażone w wymienne złącze typu SC/APC do samodzielnej wymiany, nie wymagające żadnego dodatkowego narzędzia do jego wymiany
- Ekran dotykowy o przekątnej minimum 4”
- Poręczne wymiary umożliwiające wykonanie pomiarów jedną ręką
- Waga urządzenia nie powinna przekraczać 0,5kg
- Urządzenie powinno być odporne na upadek z wysokości minimum 1m.
- Wbudowane moduły radiowej komunikacji: WiFi 802.11 oraz Bluetooth 4.2
- Czas pracy urządzenia na baterii co najmniej 10 godzin
- Urządzenie musi umożliwiać zapis wyników pomiarów na serwerze zdalnym
- Urządzenie musi posiadać funkcję diagnostyki własnego złącza pomiarowego
- Z wykonanych pomiarów powinno się w prosty sposób wygenerować raport do pliku PDF
- Wykonane pomiary powinno się w prosty sposób pobierać za pomocą dedykowanej aplikacji bezprzewodowo (Wi-Fi) , lub poprzez kabel USB

Wymagania dodatkowe :

Urządzenie musi zostać dostarczone w zestawie:

- zestaw akcesoriów czyszczących składający się z:

  - min. 1 szt. platformy zawierającej min. 200 listków chusteczek bezpyłowych oraz płaszczyznę kompensującą docisk w procesie czyszczenia czoła złącza optycznego,
  - 1 szt. rozpuszczalnika brudu (bezpiecznego dla tworzyw sztucznych) o poj. min. 200 ml z aerozolowym dozownikiem z blokadą spustu i rurką do precyzyjnych aplikacji,
  - 1 szt. czyścik automatyczny z taśmą obejmującą całą powierzchnię czoła ferruli APC/UPC/PC)
- Miękkim pokrowcem
- Adapterem USB AC
- Kablem USB
- uchwytem do paska
- Włóknem rozbiegowym jednomodowym, z złączem kompatybilnym z urządzeniem i drugim złączem SC/APC o długości minimum 20m

Ponadto, Wykonawca musi zagwarantować szkolenie dla 4 osób z obsługi urządzenia oraz z metodologii pomiarów sieci optycznych.

Gwarancja:

Warunki gwarancji nie gorsze niż warunki gwarancji producenta sprzętu.

Okres gwarancji minimum 3 lata.

Załącznik nr 2 do SWZ

……, dn. ……

PIECZĘĆ FIRMOWA WYKONAWCY:

Formularz ofertowy

Ja, niżej podpisany (a), upoważniony do reprezentowania Wykonawcy …… (pełna nazwa Wykonawcy) składam ofertę w postępowaniu nr ……., dotyczące realizacji zamówienia ……..

W związku z prowadzoną procedurą przetargową oferujemy następujące ceny netto:

Lp.	Nazwa	Ilość	Cena jedn. netto	Wartość netto	Informacje dodatkowe (nazwa, producent, nr seryjny, okres gwarancji, inne szczegóły)
Zadanie 1					
1.	Zakup przełącznika sieciowego LAN do szafy RACK 19”	1 szt.			
Zadanie nr 2					
2.	Zakup przełączników sieciowych LAN do szafy RACK 19”	2 szt.			
Zadanie nr 3					
3.	Zakup przełącznika sieciowego LAN na szynę DIN TH35mm	1 szt.			
Zadanie nr 4					
4.	Zakup przełączników sieci LAN na szynę DIN TH35mm	4 szt.			
Zadanie nr 5					
5.	Zakup za pory sieciowej nowej generacji (NGFW) do szafy RACK 19”	1 szt.			
Zadanie nr 6					
6.	Zakup urządzenia do podstawowych pomiarów i weryfikacji światłowodowych sieci optycznych	1 szt.			

1. Termin płatności wynosi …… od daty otrzymania faktury.
2. Termin realizacji zadania 1 - …….. (data)
3. Termin realizacji zadania 2 - …….. (data)
4. Termin realizacji zadania 3 - …….. (data)

5. Termin realizacji zadania 4 - …….. (data)
6. Termin realizacji zadania 5 - …….. (data)
7. Termin realizacji zadania 6 - …….. (data)
8. Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres …… dni od dnia upływu terminu składania ofert.
9. Oświadczamy, że zapoznaliśmy się z istotnymi postanowieniami Umowy, określonymi w Załączniku nr 8 do SWZ i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia Umowy zgodnej z niniejszą ofertą, na warunkach określonych w SWZ, w miejscu i terminie wyznaczonym przez Zamawiającego.
10. Oświadczamy, że w przypadku wyboru naszej oferty ceny netto nie ulegną zmianie w okresie obowiązywania umowy.
11. Oświadczamy, że posiadamy status ……. *(dużego/średniego/małego)** przedsiębiorcy w rozumieniu przepisów Ustawy z dnia 8 marca 2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.
12. Oświadczamy, że w stosunku do …….. (*nazwa Wykonawcy)** **nie** zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2022 r. poz. 835).

*należy uzupełnić

……
data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 3 do SWZ

PIECZĘĆ FIRMOWA WYKONAWCY :

……, dn. ……

Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu

Działając w imieniu …… i będąc należycie upoważnionym do jego reprezentowania oświadczam, że Wykonawca spełnia warunki udziału w postępowaniu ……., a mianowicie:

1) Posiada uprawnienia do wykonywania działalności związanej z zamówieniem,
2) Posiada niezbędną wiedzę i doświadczenie oraz potencjał techniczny, a także dysponuje personelem zdolnym do wykonania Zamówienia,
3) Znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie Zamówienia.

Wykonawca jednocześnie oświadcza, że zapoznał się z warunkami udziału w postępowaniu i akceptuje jego warunki. Wykonawca spełnia również warunki wymienione w SWZ.

……
data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 4 do SWZ

……, dn. ……

PIECZĘĆ FIRMOWA WYKONAWCY:

Oświadczenie dotyczące powiązań osobowych lub kapitałowych

W postępowaniu:

……

Oświadczam(y), że jestem(eśmy) / nie jestem(eśmy)* powiązany(ni) z Zamawiającym osobowo lub kapitałowo.

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

1. Uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej;
2. Posiadaniu, co najmniej 10 % udziałów lub akcji o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez instytucję zarządzającą programem operacyjnym;
3. Pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
4. Pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.

**niepotrzebne skreślić*

……

data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 5 do SWZ

……, dn. ……

PIECZĘĆ FIRMOWA WYKONAWCY:

Formularz dotyczący warunków RODO

Pytanie	**Odpowiedź Wykonawcy TAK/NIE (proszę wpisać właściwe)**
Czy jesteście Państwo zobowiązani zgodnie z RODO*, prowadzić rejestr operacji przetwarzania danych osobowych?	
Czy stosują Państwo zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO*, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO* lub jakikolwiek inny certyfikat? Prosimy o podanie szczegółowych informacji.	(Jeśli TAK, prosimy podać rodzaj certyfikacji)
Czy Państwa firma jest w stanie zapewnić wsparcie w przypadku: **(A)** sporządzania oceny skutków przetwarzania dla ochrony danych art. 35 RODO*, **(B)** dokonywania powiadomień o naruszeniu ochrony danych, **(C)** konsultacji z PUODO (Prezes Urzędu Ochrony Danych Osobowych) zgodnie z przepisami obowiązującego prawa (Ustawa o Ochronie Danych Osobowych z dnia 10 maja 2018 roku) oraz **(D**) realizowania praw osób, których dotyczą dane osobowe (prawo do: przenoszenia danych, zapomnienia danych, ograniczenia przetwarzania danych, dostępu do danych, sprostowania danych oraz do wniesienia sprzeciwu?	(Jeśli TAK, prosimy wypisać dla których punktów)
Czy Państwa firma jest świadoma odpowiedzialności związanej z naruszeniem przepisów dotyczących przetwarzania danych osobowych zgodnie z RODO*?	
Czy Państwa przedsiębiorstwo posiada siedziby poza terytorium UE?	(Jeśli TAK prosimy wpisać dane podmiotu)
Czy zamierzają Państwo korzystać z usług dalszych podmiotów przetwarzających (podprocesorów)?	(Jeśli TAK prosimy uzupełnić dane takich podmiotów i ich lokalizację)

* Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych zwanym dalej „RODO”).

……

data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 6 do SWZ

PIECZĘĆ FIRMOWA WYKONAWCY

……, dn. ……

Oświadczenie o niezaleganiu z płatnościami na rzecz podmiotów publicznych i prywatnych

Niniejszym oświadczam, że nie zalegam z płatnościami na rzecz podmiotów publicznych i prywatnych, a tym samym:

1) nie zalegam z opłacaniem podatków do US,

2) nie zalegam z opłacaniem składek na ubezpieczenie zdrowotne i społeczne do ZUS,

3) nie figuruję w Krajowym Rejestrze Długów,

4) nie toczą się wobec Spółki żadne postępowania sądowe lub egzekucyjne.

……

data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 7 do SWZ

PIECZĘĆ FIRMOWA WYKONAWCY

……, dn. ……

Wykaz zrealizowanych zamówień

Przystępując do udziału w postępowaniu na „……”
w celu wykazania spełniania warunku, o którym mowa w punkcie 3.2. oświadczamy, iż w okresie ostatnich trzech lat przed upływem terminu składania ofert wykonaliśmy następujące zamówienia:

Lp.	Rodzaj usługi/ w tym wskazanie zakresu i nazwy usługi	Nazwa i adres podmiotu, na rzecz którego wykonywano określoną usługę	Wartość zamówienia netto w zł	Data wykonania /odbioru (dzień - miesiąc-rok)
1.				
2.				

Do wykazu dołączono następujące dokumenty wystawione przez podmiot, na rzecz którego były wykonywane usługi potwierdzające, że zostały one wykonane należycie:

……
……
……
……

……
data i podpis upoważnionego przedstawiciela Wykonawcy

Załącznik nr 8 do SWZ

Istotne postanowienia umowne

Zawarta w dniu podpisania pomiędzy:
JSW IT SYSTEMS Spółka z o. o. z siedzibą w Jastrzębiu-Zdroju, ul. Armii Krajowej 56, wpisaną do Krajowego Rejestru Sądowego - Sąd Rejonowy w Gliwicach X Wydział Gospodarczy, pod numerem KRS: 0000083839, o kapitale zakładowym 15.665.000,00 zł, Regon: 276202273, NIP: 6331981130, BDO 000154071, którą reprezentuje:

Piotr Toś –Prezes Zarządu

zwaną dalej „**JSW ITS** ” lub „**Zamawiającym**”,
a
…… z siedzibą w……, wpisaną do Krajowego Rejestru Sądowego prowadzonego przez ……., XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS ……., o kapitale zakładowym ……. zł, Regon: ……., NIP: ……., którą reprezentuje:

……

Zwaną dalej „**Wykonawcą**”.

§ 1
PRZEDMIOT UMOWY

1. Zamawiający zleca, a Wykonawca przyjmuje do wykonania przedmiot niniejszej umowy, którym jest dostawa …… */szczegóły zostaną uzupełnione na etapie zawierania umowy z wykonawcą/.*
2. Wykonawca oświadcza, że:
   a) posiada niezbędną wiedzę, doświadczenie oraz potencjał organizacyjny zapewniający należytą i terminową realizację przedmiotu Umowy.
   b) zapoznał się z przedmiotem Umowy i nie wnosi uwag co do tych elementów pod kątem możliwości należytej i terminowej realizacji dostaw według wymagań Zamawiającego określonych niniejszą Umową,
   c) przedmiot Umowy został mu przedstawiony przez Zamawiającego w sposób jednoznaczny i wyczerpujący z uwzględnieniem jego zakresu za pomocą dostatecznie dokładnych i zrozumiałych określeń, a składając ofertę Wykonawca uwzględnił wszystkie wymagania i okoliczności mogące mieć wpływ na jej złożenie,
   d) przedmiot umowy jest fabrycznie nowy i wolny od wad fizycznych.

§ 2

KOORDYNATORZY STRON

1. Osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy:

.....

2. Osoba odpowiedzialna za realizację Umowy ze strony Zamawiającego:

.....

§ 3

TERMIN REALIZACJI

1. Dostawa przedmiotu umowy, o którym mowa w § 1 ust. 1 nastąpi w terminie ..... /szczegóły zostaną wpisane po wybraniu wykonawcy/.
2. Podstawą wystawienia faktury jest protokół odbioru bez uwag.

§ 4

WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Wynagrodzenie za realizację przedmiotu umowy określonego w § 1 ust. 1 wynosi ..... netto.
2. Wynagrodzenie określone w ust. 1 zawiera wszystkie koszty związane z realizacją przedmiotu umowy niezbędne do jej wykonania.
3. Wynagrodzenie, o którym mowa w ust. 1 będzie powiększone o podatek od towarów i usług (VAT), zgodnie ze stawką obowiązującą w dniu wystawienia faktury VAT.
4. Podstawę do wystawiania faktur stanowić będzie podpisany przez obie Strony protokół odbioru bez uwag.
5. Zapłata należności za zrealizowane dostawy zostanie dokonana przelewem, w terminie …… dni od otrzymania faktury VAT, na rachunek Wykonawcy wskazany w fakturze VAT.
6. Zamawiający zastrzega sobie prawo do zapłaty wynagrodzenia wynikającego z niniejszej Umowy przy wykorzystaniu mechanizmu podzielonej płatności.
7. Należności wynikające z Umowy w tym odsetki, nie mogą być przedmiotem jakiegokolwiek obrotu prawnego (cesja, sprzedaż) bez pisemnej zgody Zamawiającego oraz nie dopuszcza się udzielania pełnomocnictwa inkasowego do ich dochodzenia.
8. Począwszy od dnia zawarcia niniejszej Umowy Zamawiający upoważnia Wykonawcę do wystawiania faktur, faktur korygujących lub duplikatów w formie elektronicznej, zgodnie z obowiązującymi w tym zakresie przepisami prawa i doręczania ich na podany adres oraz wyraża zgodę na wysyłanie ich wyłącznie na adres poczty elektronicznej e-faktury@jswits.pl z następujących adresów e-mail: .....
9. Jeżeli Wykonawca zdecyduje się na przesyłanie faktur VAT w sposób opisany w ust. 8 to deklaruje, że jest to jedyna droga dostarczania faktur VAT do Zamawiającego za wyjątkiem przypadków wskazanych w ust. 13.
10. W przypadku przesłania faktury VAT na inny adres, niż wskazany w ust. 8, termin płatności faktury VAT określony w umowie będzie liczony od daty wpływu prawidłowo wystawionej faktury VAT na adres, o którym mowa w ust. 8.

11. Wykonawca oświadcza, że faktury elektroniczne przez niego przesyłane posiadają gwarancję autentyczności pochodzenia i integralności treści. Strony zobowiązują się do stosowania przepisów dotyczących faktur elektronicznych.
12. Za datę otrzymania faktury, faktury korygującej lub duplikatu faktury w formie elektronicznej przez Zamawiającego uznaje się datę odnotowanego faktu ich wpływu do skrzynki odbiorczej poczty elektronicznej Zamawiającego wskazanej w ust. 8.
13. Zamawiający zobowiązuje się przyjmować dokumenty, o których mowa w ust. 8 w formie papierowej w przypadku, gdy przeszkody formalne lub techniczne uniemożliwią Wykonawcy przesyłanie faktur drogą elektroniczną.
14. Strony oświadczają, iż niniejsze oświadczenie dotyczy wyłącznie faktur, faktur korygujących lub duplikatów wystawianych do tej umowy i może zostać wycofane z zachowaniem formy pisemnej w następstwie, czego Wykonawca traci prawo do wystawiania i przesyłania faktur do Zamawiającego drogą elektroniczną, począwszy od dnia następnego po otrzymaniu powiadomienia o wycofaniu zgody.
15. Strony zobowiązują się przechowywać egzemplarze faktur w formie papierowej lub elektronicznej do upływu terminu przedawnienia zobowiązań podatkowych.
16. Wykonawca, jeżeli jest czynnym podatnikiem VAT oświadcza, że numer rachunku bankowego wskazany na fakturach został umieszczony w wykazie, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług. Zamawiający zastrzega sobie prawo do wstrzymania płatności w przypadku stwierdzenia, że pomimo oświadczenia, o którym mowa powyżej doszło jednak do wskazania przez Wykonawcę rachunku niezgłoszonego organom skarbowym i nieujawnionego w stosowanych rejestrach / wykazach, w tym w szczególności w wykazie, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług. W takiej sytuacji Strony zgodnie przyjmują, że do czasu wyjaśnienia zaistniałej sytuacji okres wstrzymania się z płatnością nie będzie między Stronami traktowany jako opóźnienie w dokonaniu płatności. Ponadto Wykonawca zobowiązuje się do prawidłowego określenia mechanizmu podzielonej płatności na wystawianych przez siebie fakturach zgodnie z zapisami art.106e ust.1 pkt.18a ustawy o podatku od towarów i usług, gdy jest on wymagany.
17. Wykonawca zobowiązuje się do wpisania na każdej fakturze numeru Umowy nadanego przez Zamawiającego. Niedopełnienie tego obowiązku może spowodować zwrot faktury lub opóźnienie płatności.
18. Zamawiający/JSW IT Systems sp. z o.o. oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu przepisów Ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (Dz.U.2022 poz.893 z późn. zm.).
19. Wykonawca oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu przepisów Ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (Dz.U.2022 poz.893 z późn. zm.).

§ 5

KARY UMOWNE

1. W przypadku naruszenia z winy Wykonawcy uzgodnionego pomiędzy Stronami terminu realizacji zamówienia, Wykonawca będzie zobowiązany, na pisemne żądanie Zamawiającego, do zapłaty

kary umownej w wysokości 0,1 % wartości brutto za każdy rozpoczęty dzień zwłoki ponad ustalony termin realizacji.

2. Za odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy, Wykonawca zobowiązuje się zapłacić Zamawiającemu karę umowną w wysokości 30.000,00 złotych (słownie: trzydzieści tysięcy złotych 00/100) w terminie 10 dni od daty wystąpienia przez Zamawiającego z żądaniem zapłaty kary.
3. Zamawiający zastrzega sobie prawo odstąpienia od umowy i żądania zapłaty kary umownej wskazanej w ust. 2, w każdym czasie, w przypadku stwierdzenia niewykonania lub nienależytego wykonywania postanowień niniejszej umowy przez Wykonawcę.
4. W razie stwierdzenia uchybień w realizacji uzgodnionych warunków, Zamawiający może wezwać Wykonawcę do zmiany sposobu wykonywania umowy w terminie 7 dni od dnia ich zgłoszenia, a po bezskutecznym upływie tego terminu odstąpić od niniejszej umowy.
5. W przypadku zaistnienia sytuacji, o której mowa w ust. 4, mają zastosowanie ustalenia z § 6 ust. 4 niniejszej umowy.
6. Odstąpienie od Umowy nastąpi na podstawie oświadczenia złożonego przez Stronę uprawnioną w formie pisemnej wraz z uzasadnieniem.
7. Zamawiający zastrzega sobie prawo wskazania skutku odstąpienia „od początku” lub „na przyszłość” w oświadczeniu o odstąpieniu.
8. Zapłata kary umownej wskazanej w ust. 1 nie zwalnia Wykonawcy z realizacji przedmiotu Umowy.
9. Zapłata przez Wykonawcę kar umownych nie wyłącza prawa do dochodzenia przez Zamawiającego odpowiedzialności odszkodowawczej na zasadach ogólnych wynikających z przepisów Kodeksu cywilnego do kwoty odpowiadającej 30% łącznej wartości Umowy.
10. Zamawiający zastrzega sobie prawo do potrącania naliczonych kar umownych z wynagrodzenia należnego Wykonawcy.

§ 6

POUFNOŚĆ

1. Strony zobowiązują się wzajemnie, w okresie obowiązywania niniejszej Umowy oraz po jej zakończeniu do zachowania w poufności wszelkich informacji, jakie uzyskały w związku z wynegocjowaniem, zawarciem, wykonaniem, realizacją i rozwiązaniem Umowy, co, do których, mogą powziąć podejrzenie, iż są poufnymi informacjami lub, że jako takie są traktowane przez drugą Stronę, albo zostały określone przez tę Stronę, jako poufne.
2. Strony zobowiązują się do zachowania poufności w szczególności informacji odnośnie sprzętu, infrastruktury informatycznej, procedurach biznesowych stosowanych przez drugą Stronę, informacji stanowiących tajemnicę przedsiębiorstwa drugiej Strony oraz do dołożenia szczególnej staranności w celu ochrony danych stanowiących tajemnicę przedsiębiorstwa drugiej Strony i zapewnienie takich warunków przetwarzania danych, aby uniemożliwić dostęp do wykorzystywanych informacji osobom nieupoważnionym w czasie realizacji Umowy oraz po jej zakończeniu.
3. W razie jakichkolwiek wątpliwości, co do charakteru danej informacji, przed jej ujawnieniem lub uczynieniem dostępną, Strona zwróci się do drugiej Strony drogą mailową o wskazanie czy informację tą ma traktować, jako poufną, a do czasu uzyskania odpowiedzi drugiej Strony, będzie traktować daną informację, jako poufną.

4. Zamawiający zastrzega sobie prawo upubliczniania informacji przedstawionych w Umowie na potrzeby tworzenia raportów przekazywanych do publicznej wiadomości przez podmiot dominujący - Jastrzębską Spółkę Węglową S.A., w związku z notowaniem papierów wartościowych Jastrzębskiej Spółki Węglowej S.A. na Giełdzie Papierów Wartościowych w Warszawie S.A.
5. Zamawiający zastrzega sobie prawo przekazywania informacji przedstawionych w Umowie uprawnionym doradcom w szczególności prawnym i podatkowym, a także podmiotom działającym w Grupie Kapitałowej Jastrzębskiej Spółki Węglowej.
6. W przypadku każdego naruszenia zasad poufności, o których mowa w niniejszym paragrafie, Strona naruszająca zapłaci drugiej Stronie każdorazowo (za każdy pojedynczy przypadek naruszenia) karę umowną w wysokości 50.000,00 (słownie: pięćdziesiąt tysięcy 00/100) zł.
7. Każda ze Stron jest upoważniona do dochodzenia odszkodowania przewyższającego zastrzeżoną karę umowną na zasadach ogólnych, bez względu na przewidziane Umową limity odpowiedzialności.
8. Naruszenie obowiązku zachowania w tajemnicy informacji poufnej będzie traktowane jako podstawa rozwiązania umowy bez wypowiedzenia, a także będzie traktowane jako podstawa dochodzenia roszczeń w drodze postępowania cywilnego, na podstawie przepisów ustawy z dnia 23 kwietnia 1964r. Kodeks cywilny (Dz.U.2020, poz. 1740, z późniejszymi zmianami). Naruszenie, o którym mowa powyżej może też być podstawą złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa określonego w art. 180 i 181 Ustawy o obrocie instrumentami finansowymi.

§ 7

SIŁA WYŻSZA

1. Od obowiązków wynikających z niniejszej umowy Strony mogą być zwolnione tylko w przypadku zaistnienia „siły wyższej".
2. Za przypadki siły wyższej, które uwalniają strony od wypełnienia zobowiązań umownych na czas trwania siły wyższej oraz czas niezbędny do usunięcia jej skutków, uznaje się nieprzewidziane wydarzenia, które wystąpią niezależnie od woli stron i po zawarciu niniejszej umowy, a którym strona nie będzie mogła zapobiec, przy zastosowaniu należytej staranności, udaremniające całkowicie lub częściowo wypełnianie zobowiązań umownych, jak np. pożar, powódź, gwałtowne zjawiska atmosferyczne, trzęsienie ziemi, strajk, wojna, mobilizacja, działania wojenne wroga, rekwizycja, embargo, kwarantanna, epidemia lub zarządzenia władz. Siła wyższa oznacza także zagrożenia wodne, pożarowe lub każde inne, występujące w podziemnych wyrobiskach zakładów górniczych Zamawiającego, związane zwłaszcza z tąpnięciami, wybuchami metanu lub pyłu węglowego, wyrzutami gazów lub skał, prowadzeniem akcji ratowniczych, które uniemożliwiają lub znacząco ograniczają wykonanie umowy.
3. Nie uznaje się za siłę wyższą braku siły roboczej, materiałów i surowców, chyba że jest to spowodowane siłą wyższą.
4. O zaistnieniu okoliczności uznanych za siłę wyższą strony zobowiązane są niezwłocznie się powiadomić.
5. Niezwłocznie po ustaniu siły wyższej, Strony przystąpią do dalszego wykonania umowy.
6. Określony w umowie termin realizacji umowy ulega wydłużeniu o czas działania siły wyższej oraz czas niezbędny do usunięcia skutków działania siły wyższej.

§ 8

ETYKA BIZNESU

Wykonawca oświadcza, że zapoznał się z obowiązującym w Grupie JSW, w skład której wchodzi Zamawiający, „Kodeksem Etyki JSW”, którego treść została udostępniona na stronie www.jsw.pl/odpowiedzialny-biznes/kodeks-etyki-grupy-jsw/ i zobowiązuje się, że w związku z realizacją niniejszej umowy będzie przestrzegać zasad opisanych w ww. Kodeksie, oraz że standardów tych przestrzegać będą jego podwykonawcy oraz wszelkie inne osoby przy pomocy których wykonuje umowę, jak również osoby, którym powierza wykonanie umowy (w całości lub w części). Ponadto Wykonawca zobowiązuje się do zapobiegania i niepodejmowania działań, które mogłyby powodować naruszenie tych zasad przez jego pracowników. Wykonawca zapewni zgodność swoich działań z powyższymi zasadami i na żądanie Zamawiającego niezwłocznie poinformuje o stosowanych w tym zakresie procedurach. Za wszelkie działania lub zaniechania stanowiące naruszenie powyższych obowiązków przez podwykonawców, osoby przy pomocy których Wykonawca wykonuje umowę, jak również osoby, którym powierza wykonanie Umowy (w całości lub w części), Wykonawca ponosi odpowiedzialność jak za działania własne.

§ 9

PRZETWARZANIE DANYCH OSOBOWYCH STRON

1. Na potrzeby realizacji niniejszej Umowy Strony, jako niezależni administratorzy danych przekazywać będą sobie nawzajem dane osobowe swoich reprezentantów lub przedstawicieli oraz innych osób w zależności od potrzeb wynikających z postanowień niniejszej Umowy.
2. Podstawą prawną przetwarzania w/w danych jest prawnie uzasadniony interes każdej ze Stron, o którym mowa w art. 6 ust. 1 lit. f 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 – zwane dalej RODO) związany z realizacją wykonania postanowień niniejszej Umowy.
3. Strony zobowiązują się do poinformowania osób, o których mowa w ust. 1, o konieczności przekazania ich danych na potrzeby realizacji niniejszej Umowy, w tym o celu i zakresie przekazywanych danych. Strona przekazująca dane ma również obowiązek przekazać osobom informację na temat przetwarzania ich danych zgodnie z RODO przez Stronę otrzymującą dane, w sytuacji otrzymania od niej takich informacji.
4. Informacja dotycząca przetwarzania danych osobowych (klauzula informacyjna) przez Zamawiającego znajduje się Załączniku do niniejszej Umowy.

§10

KLAUZULE ANTYKORUPCYJNE

Odrzucenie korupcji

Wykonawca oświadcza, że w swojej działalności nie stosuje i nie toleruje korupcji, łapownictwa oraz wszelkich innych form wywierania wpływu, które mogą być sprzeczne z prawem lub dobrymi obyczajami. Wykonawca oświadcza, że zapoznał się z obowiązującą w JSW IT Systems sp. z o.o.

„Polityką antykorupcyjną Grupy Kapitałowej JSW” oraz „Procedurą zgłaszania nieprawidłowości w Grupie Kapitałowej JSW”, których treść została udostępniona na stronie [https://www.jswits.pl/o-nas/compliance] i zobowiązuje się, że w związku z realizacją niniejszej umowy będzie przestrzegać zasad opisanych w ww. Polityce i Procedurze, oraz że standardów tych przestrzegać będą jego podwykonawcy oraz wszelkie inne osoby przy pomocy których wykonuje umowę. W celu uniknięcia wątpliwości, powyższe nie stanowi zgody na realizację przedmiotu umowy przez Wykonawca z udziałem podwykonawców lub innych osób trzecich, o ile z innych postanowień umowy lub z jej istoty wynika obowiązek realizowania przedmiotu umowy bez udziału podwykonawców lub innych osób trzecich.

Zobowiązanie do niepodejmowania działań korupcyjnych

Wykonawca zobowiązuje się, że członkowie kadry kierowniczej i pracownicy nie będą stosować i tolerować korupcji, łapownictwa, jak również żadnych innych form wywierania wpływu, które są sprzeczne z prawem lub dobrymi obyczajami, w tym w szczególności nie będą (bezpośrednio lub w sposób dorozumiany) oferować, obiecywać, udzielać, upoważniać, zabiegać o korzyści lub przyjmować jakichkolwiek nienależnych korzyści (lub nie będą sugerowali, że dokonają lub mogą dokonać takiej czynności w dowolnym czasie w przyszłości) w jakikolwiek sposób związany z umową oraz że podjął uzasadnione środki, aby uniemożliwić podwykonawcom, agentom lub jakimkolwiek innym osobom trzecim, podlegającym jej kontroli lub decydującemu wpływowi, dokonanie takich czynności.

Zobowiązanie do udzielenia informacji

Wykonawca zobowiązuje się do udzielenia drugiej stronie informacji w zakresie niezbędnym do wykazania, że Wykonawca wywiązuje się z określonych w niniejszej umowie obowiązków dotyczących niepodejmowania działalności korupcyjnej i zapobiegania korupcji, w terminie 14 (czternastu) dni od dnia doręczenia wezwania drugiej stronie.

Procedura naprawcza

Jeżeli Zamawiający uprawdopodobni, że Wykonawca dopuściło się naruszenia lub kilku powtarzających się naruszeń postanowień obowiązków dotyczących niepodejmowania działalności korupcyjnej i zapobiegania korupcji, Zamawiający powiadomi o tym Wykonawca i zażąda podjęcia w rozsądnym terminie niezbędnych działań naprawczych oraz poinformowania o takich działaniach. Jeżeli nie zostaną podjęte skuteczne działania naprawcze Zamawiający może, według własnego uznania, zawiesić Umowę lub ją wypowiedzieć, przy założeniu, że wszystkie kwoty i świadczenia należne na mocy Umowy w momencie jej zawieszenia lub wypowiedzenia pozostaną wymagalne i należne, w zakresie dopuszczalnym obowiązującymi przepisami prawa.

Odpowiedzialność

Za szkodę poniesioną przez Zamawiającego wynikającą z niewykonania lub nienależytego wykonania określonych w niniejszej umowie obowiązków dotyczących niepodejmowania działalności korupcyjnej i zapobiegania korupcji oraz innych form wywierania wpływu, które są sprzeczne z prawem lub dobrymi obyczajami Wykonawca ponosi odpowiedzialność na zasadach ogólnych, niezależnie od limitów i ograniczeń określonych w Umowie.

§11

KLAUZULA SALWATORYJNA

Jeżeli którekolwiek z postanowień niniejszej umowy okaże się z jakiegokolwiek powodu nieważne, sprzeczne z prawem lub nieskuteczne, legalność i wykonalność pozostałych postanowień nie będzie w żaden sposób naruszona lub osłabiona, a Strony zobowiązują się uzgodnić postanowienie zastępujące, mające moc prawną i skutek możliwie najbardziej zbliżony do postanowienia zastępowanego.

§ 12

KLAUZULA SANKCYJNA

1. Wykonawca oświadcza, że według jego najlepszej wiedzy, na niego, jak również jego jednostkę dominującą w rozumieniu ustawy o rachunkowości, jego beneficjentów rzeczywistych w rozumieniu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, jak również na jego podmioty zależne w rozumieniu ustawy o podatku dochodowym od osób prawnych, nie zostały nałożone żadne środki ograniczające, jak również wszelkie inne sankcje, restrykcje oraz zakazy wynikające z przepisów powszechnie obowiązującego prawa, a w szczególności te o których mowa w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz ustawie o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego i nie występują jakiekolwiek okoliczności przewidziane we wskazanych powyżej przepisach uniemożliwiające realizację niniejszej umowy.
2. Wykonawca oświadcza, że jest świadomy obowiązku przestrzegania wszelkich obowiązujących przepisów prawa w zakresie zakazu współpracy (choćby pośrednio) z państwami i podmiotami, na które nałożone zostały środki ograniczające, jaki i handlu towarami objętymi sankcjami bez odpowiednich zezwoleń. W szczególności Wykonawca gwarantuje, że nie łamie żadnych sankcji nakładanych przez ustawodawstwo krajowe i unijne, jak również zobowiązany jest do natychmiastowego zawiadomienia JSW ITS o wystąpieniu w trakcie realizacji niniejszej umowy okoliczności przewidzianych w ust. 1, które uniemożliwiają dalszą realizację niniejszej umowy.
3. JSW ITS na każdym etapie realizacji niniejszej umowy uprawniony będzie wezwać Wykonawcę do złożenia oświadczenia, że nie występują okoliczności, przewidziane w ust. 1. W odpowiedzi na wezwanie Wykonawcy zobowiązany będzie złożyć pisemne oświadczenie w terminie wyznaczonym przez JSW ITS.
4. Zaniechanie realizacji przez Wykonawcę obowiązków przewidzianych w ust. 2 lub 3 albo złożenie oświadczenia niezgodnego ze stanem faktycznym będzie niewykonaniem niniejszej umowy z przyczyn leżących po stronie Wykonawcy.
5. W przypadku naruszenia przez Wykonawcę obowiązków przewidzianych w ust. 2 lub 3 albo złożenia oświadczenia niezgodnego ze stanem faktycznym, JSW ITS uprawniony będzie do skorzystania ze wskazanych poniżej uprawień:
   a) odstąpienia od umowy na zasadach określonych w niniejszej umowie oraz obciążenia Wykonawcy przewidzianą w niniejszej umowie karą umowną za rozwiązanie umowy,
   b) odmowa realizacji przedmiotu Umowy, w szczególności zamówionych, a niezrealizowanych jeszcze dostaw lub usług, nie dłużej jednak niż do czasu ustania okoliczności, z powodów których nastąpiła odmowa,

c) wstrzymanie wszystkich wymagalnych i niewymagalnych świadczeń pieniężnych i niepieniężnych wobec Wykonawcy, nie dłużej jednak niż do czasu ustania okoliczności, z powodu których nastąpiło wstrzymanie,

d) rozwiązania umowy bez zachowania okresu wypowiedzenia na zasadach określonych w niniejszej umowie oraz obciążyć Wykonawcę przewidzianą w niniejszej umowie karą umowną za rozwiązanie umowy.

6. Wybór uprawnienia, o jakim mowa w ust. 5 zostaje pozostawiony do wyłącznej decyzji JSW ITS.
7. W przypadku wykonania uprawnień, o których mowa w ust. 5 przez JSW ITS, Wykonawcy nie przysługują jakiekolwiek roszczenia w stosunku do JSW ITS zarówno w zakresie poniesionej z tego tytułu szkody, w tym roszczenie o dalszą realizację niniejszej umowy, jak i odstąpienia od umowy/rozwiązania umowy bez zachowania okresu wypowiedzenia.
8. Wykonawca jest zobowiązany do naprawienia w pełnym zakresie szkody, którą JSW ITS poniesie wskutek naruszenia przez Wykonawcę jakichkolwiek środków ograniczających, jak również wszelkich innych sankcji restrykcji oraz zakazów, przewidzianych w powszechnie obowiązujących przepisach prawa krajowego i unijnego.

§ 13
ZGODNOŚĆ Z NORMAMI ISO

1. W związku z funkcjonującym w Jastrzębskiej Spółce Węglowej S.A. Zintegrowanym Systemem Zarządzania zgodnie z aktualnymi wymaganiami norm PN-EN ISO 9001 (system zarządzania jakością), PN-EN ISO 14001 (system zarządzania środowiskowego), PN-ISO 45001 (system zarządzania bhp) oraz PN-ISO/IEC 27001 (system zarządzania bezpieczeństwem informacji), Wykonawca oświadcza, że przed przystąpieniem do prac objętych przedmiotem umowy zapozna się z zasadami obowiązującymi w tym zakresie w Jastrzębskiej Spółce Węglowej S.A., w tym z Polityką Zintegrowanego Systemu Zarządzania JSW S.A. oraz znaczącymi aspektami środowiskowymi, oraz że w związku z realizacją umowy będzie przestrzegał tych zasad. Wykonawcy nie będą przysługiwały jakiekolwiek szczególne uprawnienia zastrzeżone dla pracowników Jastrzębskiej Spółki Węglowej S.A. wynikające ze wskazanych powyżej regulacji.
2. Wykonawca zobowiązany jest do realizacji umowy zgodnie z przepisami prawa ze szczególnym uwzględnieniem przepisów BHP oraz z zachowaniem zasady minimalizacji szkodliwego oddziaływania na środowisko.
3. Wykonawca zobowiązany jest do uprzedniego zapoznania z zasadami, o których mowa w punkcie 1) i 2) powyżej wszystkie osoby, przy pomocy których będzie on realizował umowę, oraz zobowiązania tych osób do ich przestrzegania, jak również zobowiązany jest na wezwanie JSW ITS do wykazania realizacji powyższego obowiązku.
4. Informacje dotyczące zasad, o których mowa w punkcie 1) i 2) powyżej dostępne są na stronie internetowej https://www.jsw.pl/o-nas/systemy-zarzadzania, jak również u Pełnomocnika Zarządu ds. Zintegrowanego Systemu Zarządzania i Zarządzania Ryzykiem Jastrzębskiej Spółki Węglowej S.A. w Biurze Zarządu Jastrzębskiej Spółki Węglowej S.A. oraz u Pełnomocnika Dyrektora Zakładu Jastrzębskiej Spółki Węglowej S.A. ds. Zintegrowanego Systemu Zarządzania.
5. JSW ITS jest zobowiązany do pisemnego poinformowania Wykonawcy o wszelkich zmianach w zakresie zasad o których mowa w punkcie 1) i 2) powyżej. Zmiana tych zasad nie powoduje

konieczności zawarcia aneksu do umowy, jednakże rodzi po stronie Wykonawcy powstanie obowiązku, o którym mowa w punkcie 3) powyżej.

§14

POSTANOWIENIA KOŃCOWE

1. Umowa wchodzi w życie z dniem podpisania.
2. Umowa zawarta jest na okres ……. od daty jej podpisania przez Strony.
3. Każdej ze Stron przysługuje prawo do jej rozwiązania z zachowaniem 3 miesięcznego terminu wypowiedzenia.
4. Zamawiającemu przysługuje prawo do rozwiązania Umowy w każdym czasie, bez wypowiedzenia, gdy Wykonawca nie wywiązuje się ze swoich zobowiązań wynikających z Umowy, mimo uprzedniego pisemnego wezwania do zmiany sposoby wykonywania i wyznaczenia dodatkowego terminu 7 dni. Oświadczenie o rozwiązaniu Umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia
5. W przypadku rozwiązania Umowy z przyczyn, o których mowa w ust. 4 powyżej, Wykonawcy nie przysługuje prawo do dochodzenia roszczeń z tego tytułu.
6. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie odpowiednie przepisy Kodeksu Cywilnego.
7. Właściwym do rozpoznania sporów wynikłych na tle realizacji niniejszej Umowy jest Sąd właściwy miejscowo według siedziby Zamawiającego.
8. Zamawiający dopuszcza zmiany nie prowadzące do zmiany charakteru umowy, o ile konieczność zmiany umowy spowodowana jest okolicznościami, których Zamawiający, działając z należytą starannością, nie mógł przewidzieć
9. Zmiana postanowień niniejszej Umowy może nastąpić za zgodą Stron wyrażoną na piśmie, pod rygorem nieważności.
10. Integralną część Umowy stanowi Załącznik nr 1 (*zgodny z punktem 5 SWZ, zostanie uzupełniony po wyborze Wykonawcy*) – Klauzula informacyjna RODO

Zamawiający **Wykonawca**