25 lat
Agencja Restrukturyzacji
i Modernizacji Rolnictwa
Al. Jana Pawła II 70, 00-175 Warszawa

Adres korespondencyjny:

Agencja Restrukturyzacji i Modernizacji Rolnictwa
ul. Poleczki 33
02-822 Warszawa

numer referencyjny sprawy: DPiZP.2610.27.2019

Specyfikacja Istotnych Warunków Zamówienia

w postępowaniu o udzielenie zamówienia publicznego
o wartości powyżej 144 000 €
prowadzonym w trybie przetargu nieograniczonego

na:
„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"

wszczętym na podstawie ustawy z dnia 29 stycznia 2004 r.
- Prawo zamówień publicznych (tj.: Dz. U. z 2018 r. poz. 1986 z późn. zm.)

INFORMACJE OGÓLNE DOTYCZĄCE PROWADZONEGO POSTĘPOWANIA

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w języku polskim. Komunikacja między Zamawiającym a Wykonawcami w niniejszym postępowaniu odbywa się przy użyciu środków komunikacji elektronicznej, tj. „Platformy Zakupowej" dostępnej pod adresem https://platformazakupowa.pl/pn/arimr (dalej: „Platforma Zakupowa").

2. Informacje i dokumenty związane z przedmiotowym postępowaniem zostały zamieszczone w zakładce „Postępowania". W celu zapoznania się z zamieszczonymi informacjami lub dokumentami należy przejść na formularz postępowania.

3. Poniżej Zamawiający przedstawia wymagania techniczno-organizacyjne związane z udziałem Wykonawców w postępowaniu o udzielenie zamówienia publicznego:

   1) Złożenie oferty możliwe jest przez Wykonawców, którzy posiadają konto na Platformie Zakupowej oraz przez Wykonawców nie posiadających konta na Platformie Zakupowej. W celu założenia konta na Platformie Zakupowej należy wybrać zakładkę „Zaloguj się" w kolejnym kroku należy wybrać „Załóż konto", następnie należy wypełnić formularze i postępować zgodnie z poleceniami wyświetlającymi się na ekranie monitora. W przypadku Wykonawców niezalogowanych w celu złożenia oferty niezbędne jest podanie adresu e-mail (na który wysłane będzie potwierdzenie złożenia oferty), nr NIP oraz nazwy firmy, nieobowiązkowo nr telefonu.

   2) Złożenie oferty oraz oświadczenia, o którym mowa w art. 25a z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (tj.: Dz. U. z 2018 r. poz. 1986 z późn. zm.; dalej: „ustawa"), w tym Jednolitego Europejskiego Dokumentu Zamówienia składanych w trakcie toczącego się postępowania wymaga od Wykonawcy posiadania kwalifikowanego podpisu elektronicznego.

   3) Wykonawca składa ofertę, która w przypadku prawidłowego złożenia oferty zostaje automatycznie zaszyfrowana przez system. Nie jest możliwe zapoznanie się z treścią złożonej oferty przed upływem terminu otwarcia ofert.

   4) Podpisanie dokumentów w formie skompresowanej poprzez opatrzenie całego pliku jednym podpisem kwalifikowanym jest równoznaczne z poświadczaniem za zgodność z oryginałem wszystkich elektronicznych kopii dokumentów. Dokumenty, co do których wymagana jest forma oryginału, muszą zostać podpisane indywidualnie (każdy z nich) kwalifikowanym podpisem elektronicznym. Podpisanie skompresowanego pliku, w którym umieszczono dokument w formie oryginału nie stanowi podpisania tego dokumentu.

4. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia Prezesa Rady Ministrów w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępnienia i przechowywania dokumentów elektronicznych (Dz. U. z 2017 r. poz. 1320; dalej: „Rozporządzenie w sprawie środków komunikacji"), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na Platformie Zakupowej, tj.:

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

   2) komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,

   3) zainstalowana dowolna przeglądarka internetowa; w przypadku Internet Explorer minimalnie wersja 10.0.,

   4) włączona obsługa JavaScript,

   5) zainstalowany program Adobe Acrobat Reader, lub inny obsługujący format plików .pdf.

5. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalne formaty przesyłanych danych, tj. plików o wielkości do 75 MB. Zalecany format: .pdf.

6. Zamawiający, zgodnie z § 3 ust. 3 Rozporządzenia w sprawie środków komunikacji, określa informacje na temat kodowania i czasu odbioru danych, tj.:

   1) Plik załączony przez Wykonawcę na Platformie Zakupowej i zapisany nie jest widoczny dla Zamawiającego, gdyż jest w systemie jako zaszyfrowany. Możliwość otworzenia pliku dostępna jest dopiero po odszyfrowaniu przez system, co następuje po terminie otwarcia ofert,

   2) Oznaczenie czasu odbioru danych przez Platformę stanowi przypiętą do oferty elektronicznej datę oraz dokładny czas (hh:mm:ss), znajdujące się w kolumnie dotyczącej danej oferty, w sekcji - "Data złożenia oferty".

7. Zamawiający, zgodnie z § 4 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalny format kwalifikowanego podpisu elektronicznego jako:

   1) dokumenty w formacie .pdf zaleca się podpisywać formatem PAdES;

   2) dopuszcza się podpisanie dokumentów w formacie innym niż .pdf, wtedy zaleca się użyć formatu XAdES.

8. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z Platformy Zakupowej, określone w Regulaminie zamieszczonym na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr w zakładce „Regulamin" oraz uznaje go za wiążący.

9. Zamawiający informuje, że instrukcje korzystania z Platformy Zakupowej dotyczące w szczególności logowania, pobrania dokumentacji, składania wniosków o wyjaśnienie treści siwz, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu Platformy Zakupowej znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem https://platformazakupowa.pl/pn/arimr.

10. Korzystanie z Platformy Zakupowej jest bezpłatne. W celu ułatwienia Wykonawcom korzystania z Platformy Zakupowej operator platformy uruchomił Centrum Wsparcia Klienta, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mai: cwk@platformazakupowa.pl

Rozdział I. Przedmiot zamówienia.

I.1. Opis przedmiotu zamówienia.

1. Kod Wspólnego Słownika Zamówień (CPV).
   Główny kod: 32420000 – 3 [Urządzenia sieciowe]
2. Przedmiotem zamówienia jest:
   2.1. zakup wraz z dostawą 2 sztuk fabrycznie nowych, takich samych, nienoszących śladów uprzedniego używania urządzeń Firewall wraz z systemem zarządzania i Oprogramowaniem niezbędnym do zachowania wyspecyfikowanej funkcjonalności (dalej „Sprzęt IT"), spełniających co najmniej parametry i funkcjonalności określone w Załączniku nr 1 do wzoru umowy wraz z załącznikami, stanowiącej załącznik nr 6 do specyfikacji istotnych warunków zamówienia [dalej: siwz];
   2.2. wykonanie Wdrożenia Sprzętu IT, zgodnie z zasadami określonymi we wzorze umowy wraz z załącznikami, stanowiącej załącznik nr 6 do siwz;
   2.3. wykonanie Dokumentacji powykonawczej i dostarczenie jej w formie papierowej i elektronicznej do akceptacji i odbioru Zamawiającemu;
   2.4. świadczenie Serwisu gwarancyjnego dla Sprzętu IT, z czasem naprawy 6 godzin, przez okres 36 miesięcy na warunkach opisanych we wzorze umowy wraz z załącznikami, stanowiącej załącznik nr 6 do siwz;
   2.5. zapewnienie przez Wykonawcę 500 (słownie: pięćset) godzin konsultacji w czasie trwania Serwisu gwarancyjnego. Konsultacje będą obejmowały analizy, audyty oraz rekomendację dot. Sprzętu IT lub Oprogramowania, jak również wszelkiego rodzaju prace rekonfiguracyjne Sprzętu IT lub Oprogramowania oraz pomoc przy pracach technicznych przeprowadzanych przez Zamawiającego, w Lokalizacjach Zamawiającego. Konsultacje będą świadczone w języku polskim.
   2.6. W ramach konsultacji technicznych Wykonawca na wniosek Zamawiającego przeprowadzi warsztaty lub prezentacje dot. wskazanego elementu Sprzętu IT oraz Oprogramowania w Centrali Zamawiającego przy ul. Poleczki 33 w Warszawie. Czas dojazdu do Wykonawcy nie będzie wliczony jako wykorzystanie dostępnej puli godzin
3. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych we wzorze Umowy wraz z załącznikami stanowiącym Załącznik nr 6 do SIWZ.

I.2. Opis części zamówienia.

Zamawiający nie dopuszcza składania przez Wykonawcę ofert częściowych w rozumieniu art. 2 pkt 6) ustawy.

I.3. Powierzenie Podwykonawcy wykonania części zamówienia.

1. Zamawiający dopuszcza powierzenie Podwykonawcom wykonania części zamówienia.
2. Wykonawca zobowiązany jest do wskazania w ofercie części zamówienia, której wykonanie zamierza powierzyć Podwykonawcy oraz do podania firm Podwykonawców.

I.4. Pozostałe istotne elementy związane z przedmiotem zamówienia.

1. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 7) ustawy.
2. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu art. 2 pkt 7) ustawy.
3. Zamawiający nie przewiduje zawarcia umowy ramowej na podstawie art. 99 ustawy, jak również nie przewiduje przeprowadzenia aukcji elektronicznej.
4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
5. Wszelkie rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).

Rozdział II. Termin wykonania zamówienia.

Zamawiający wymaga realizacji zamówienia w następujących terminach:

1. Zamawiający wymaga dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenia w lokalizacjach COPD (Centralne Ośrodki Przetwarzania Danych Zamawiającego) nie później niż w terminie do 20 Dni Roboczych* od dnia zawarcia Umowy.
2. Wykonawca powiadomi, w formie pisemnej, Zamawiającego o terminie dostarczenia Sprzętu IT wraz z Oprogramowaniem, i Dokumentów oraz o terminie rozpoczęcia Wdrożenia w poszczególnych lokalizacjach COPD, z wyprzedzeniem co najmniej 5 Dni Roboczych. W terminie do 2 Dni Roboczych Zamawiający potwierdzi wskazany termin lub wskaże inny, jednak nie później niż 2 Dni Robocze od daty otrzymania przez Zamawiającego ww. powiadomienia.
3. Serwis gwarancyjny świadczony będzie przez Wykonawcę przez okres 36 miesięcy od dnia podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 wzoru Umowy.

UWAGA:

**W przypadku, gdy Wykonawca w ramach kryterium oceny ofert (patrz ROZDZIAŁ XI siwz) wskaże w Formularzu Ofertowym terminy inne niż wymagane powyżej w pkt 1 termin ten zostanie wpisany odpowiednio do wzoru Umowy.*

Rozdział III. Warunki udziału w postępowaniu oraz podstawy wykluczenia.

1. O zamówienie mogą ubiegać się Wykonawcy, którzy:
   1.1. Nie podlegają wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12 – 23 ustawy oraz art. 24 ust. 5 ustawy;
   1.2. Spełniają warunki udziału w postępowaniu w zakresie zdolności zawodowej. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:
      1.2.1. wykonał, w okresie ostatnich trzech (3) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie,

      co najmniej 2 (dwie) dostawy urządzeń typu Firewall (urządzenia pełniące funkcje zapory ogniowej), wraz z wdrożeniem, o wartości każdej z nich nie mniejszej niż 300 000,00 zł brutto (słownie: trzysta tysięcy złotych 00/100).

UWAGA 1

Jeżeli wartość dostawy wskazanej w wykazie jest podana w walucie innej niż PLN, Wykonawca zobowiązany jest, na potrzeby niniejszego postępowania, dokonać przeliczenia jej wartości na PLN wg średniego kursu NBP (www.nbp.pl tabela A – tabela kursów średnich walut obcych) z dnia zakończenia dostawy o zakresie jak wyżej wraz z podaniem kursu oraz daty jego obowiązywania (zgodnie z tabelą A – tabela kursów średnich walut obcych) wg których dokonano przeliczenia; w przypadku dostaw nadal realizowanych - wg tabeli kursów średnich walut obcych z dnia rozpoczęcia realizacji danej dostawy.

1.2.2. dysponuje następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem niezbędnymi do wykonania zamówienia, tj.: dysponuje **co najmniej jedną osobą, która posiada:**

1.2.2.1. co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.2.1. z wyłączeniem wartości zamówień;

1.2.2.2. certyfikat Cisco Certified Internetwork Expert (CCIE) Security lub równoważny.

UWAGA 2

Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:

1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:
   i. analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,
   ii. analogiczny stopień poziomu kompetencji,
   iii. analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,
2) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).

UWAGA 3

Zamawiający wymaga, aby Wdrożenie objęte przedmiotem zamówienia odbywało się co najmniej przez osobę wykazaną przez Wykonawcę na potwierdzenie spełniania opisanego przez Zamawiającego warunku udziału w postępowaniu w zakresie dysponowania osobami zdolnymi do realizacji zamówienia

UWAGA 4

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia:

1) brak podstaw wykluczenia, o których mowa w pkt 1.1 musi spełniać każdy Wykonawca z osobna,
2) warunki udziału w postępowaniu określone w pkt 1.2 musi spełniać co najmniej jeden Wykonawca lub wszyscy Wykonawcy łącznie.

2. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w Rozdziale IV niniejszej SIWZ. Z treści załączonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.
3. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 25a ust. 1 ustawy, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
4. Jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
5. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę:
   5.1. na podstawie art. 24 ust. 1 pkt 12 – 23 ustawy,
   5.2. na podstawie art. 24 ust. 5 ustawy, tj.:
      5.2.1. art. 24 ust. 5 pkt 1 ustawy, tj. Wykonawcę w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2017 r. poz. 1508 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2017 r. poz. 2344 z późn. zm.),
      5.2.2. art. 24 ust. 5 pkt 2 ustawy, tj. Wykonawcę który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych,
      5.2.3. art. 24 ust. 5 pkt 3 ustawy, tj. jeżeli Wykonawca lub osoby, o których mowa w art. 24 ust. 1 pkt 14 ustawy, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2 – 4 ustawy z:
         5.2.3.1. Zamawiającym,
         5.2.3.2. osobami uprawnionymi do reprezentowania Zamawiającego,
         5.2.3.3. członkami komisji przetargowej,
         5.2.3.4. osobami, które złożyły oświadczenie, o których mowa w art.17 ust. 2a ustawy,
         - chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu;
      5.2.4. art. 24 ust. 5 pkt 4 ustawy, tj. Wykonawcę który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 ustawy, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania,

5.2.5. art. 24 ust. 5 pkt 5 ustawy, tj. Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3 000 złotych,

5.2.6. art. 24 ust. 5 pkt 6 ustawy, tj. Wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3 000 złotych,

5.2.7. art. 24 ust. 5 pkt 7 ustawy, tj. Wykonawcę, wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3 000 złotych,

5.2.8. art. 24 ust. 5 pkt 8 ustawy, tj. Wykonawcę który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w ust. 1 pkt 15 ustawy, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

6. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania.
7. Zamawiający informuje, że zgodnie z procedurą wskazaną w art. 24aa ustawy, najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza (na podstawie kryteriów oceny ofert określonych w SIWZ) nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

Rozdział IV. Zawartość ofert, wykaz oświadczeń lub dokumentów potwierdzających brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu.

W zakresie nieuregulowanym postanowieniami SIWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r. poz. 1126 ze zm. dalej: „Rozporządzenie w sprawie rodzajów dokumentów").

IV.1. Zawartość ofert.

1. Ofertę należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SIWZ) **za pośrednictwem Platformy Zakupowej**.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty:
   2.1. Pełnomocnictwo do podpisania oferty pod rygorem nieważności w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym przez osobę/y upoważnione do reprezentacji wskazane we właściwym rejestrze, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym. Zamawiający dopuszcza złożenie elektronicznej kopii pełnomocnictwa poświadczonej przez notariusza.
   2.2. Dowód wniesienia wadium - dokument wadium, oryginał gwarancji/poręczenia, jeżeli Wykonawca wnosi wadium w innej formie niż pieniądz opatrzone kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). W przypadku wniesienia wadium w innej formie niż pieniądz, powinno ono obowiązywać przez cały okres związania ofertą.
   2.3. Zobowiązanie podmiotu trzeciego lub inny dokument potwierdzający, że Wykonawca będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym przez osobę upoważnioną do reprezentacji wskazane we właściwym rejestrze. Zapisy Rozdziału IV.5 SIWZ stosuje się odpowiednio.
   2.4. Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia (dalej: „JEDZ") sporządzone zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 Dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE. Dokument JEDZ należy złożyć pod rygorem nieważności w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym.
   2.5. Ogólnodostępny dokument producenta lub wyciąg z tego dokumentu, wraz ze wskazaniem dokładnego miejsca w dokumencie potwierdzającego spełnianie wymagań określonych w Rozdziale XI, pkt 1.2 SIWZ i oferowanych przez wykonawcę w Tabeli nr 2 Formularza ofertowego, **jeżeli wykonawca oferuje dodatkowe parametry techniczne punktowane w ramach kryterium oceny ofert „Parametry techniczne Sprzętu IT"**.

IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia.

1. Wykonawca wypełnia JEDZ, tworząc dokument w postaci elektronicznej. Wykonawca może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu w postaci elektronicznej.
   1.1. Zamawiający udostępnia Wykonawcom plik, w formacie xml, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 7 do SIWZ.
   1.2. Zamawiający informuje, że pod adresem: https://espd.uzp.gov.pl Urząd Zamówień Publicznych udostępnił nieodpłatne narzędzie umożliwiające zamawiającym i wykonawcom utworzenie, wypełnienie i ponowne wykorzystanie standardowego formularza JEDZ (JEDZ/ESPD) w wersji elektronicznej (eESPD).
2. Oświadczenia podmiotów składających ofertę wspólnie oraz podmiotów udostępniających potencjał składane na formularzu JEDZ muszą mieć formę dokumentu w postaci elektronicznej podpisanego kwalifikowanym podpisem elektronicznym przez każdy z tych podmiotów w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 22 ust. 1 ustawy.
3. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez Wykonawcę, jest Platforma Zakupowa.
4. Dokument elektroniczny JEDZ należy złożyć w formacie .pdf).

5. Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 26 ust. 3 ustawy; W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie o którym mowa w Rozdziale IV.1. pkt 2.4. SIWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.
6. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu składa także oświadczenia JEDZ, o którym mowa w Rozdziale IV.1. pkt 2.4. SIWZ, dotyczące tych podmiotów.

IV.3. Oświadczenia lub dokumenty, potwierdzające spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

1. Wykonawca obowiązany jest w terminie **3 dni od dnia zamieszczenia na stronie internetowej** Zamawiającego (Platformie Zakupowej) - www.platformazakupowa.pl/pn/arimr **informacji**, o których mowa w art. 86 ust. 5 ustawy, **do przekazania Zamawiającemu oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy**. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Wzór oświadczenia stanowi Załącznik nr 3 do SIWZ.
2. Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów podpisanych kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności w poniższym zakresie:
   2.1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
      2.1.1. informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy oraz, odnośnie skazania za wykroczenie na karę aresztu, w zakresie określonym przez zamawiającego na podstawie art. 24 ust. 5 pkt 5 i 6 ustawy, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,
      2.1.2. zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
      2.1.3. zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
      2.1.4. odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy,
      2.1.5. oświadczenia 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 albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności,
      2.1.6. oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,
      2.1.7. oświadczenia Wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2018 r. poz. 1445 z późn. zm.),
      2.1.8. oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu skazującego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym w art. 24 ust. 5 pkt 5 i 6 ustawy,
      2.1.9. oświadczenia Wykonawcy o braku wydania wobec niego ostatecznej decyzji administracyjnej o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym w zakresie określonym w art. 24 ust. 5 pkt 7 ustawy.
   2.2. potwierdzenia spełniania warunków udziału w postępowaniu dotyczących zdolności zawodowej:
      2.2.1. wykazu dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. Wzór oświadczenia stanowi Załącznik nr 4 do SIWZ.
      2.2.2. wykazu osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego wraz z informacjami na temat ich kwalifikacji zawodowych niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. Wzór oświadczenia stanowi Załącznik nr 5 do SIWZ.

2.3. potwierdzenia spełniania przez oferowane dostawy wymagań:
2.3.1. ogólnodostępnego dokumentu producenta lub wyciągu z tego dokumentu, wraz ze wskazaniem dokładnego miejsca w dokumencie potwierdzającego spełnianie wymagań dla każdego z parametrów **określonych w załączniku nr 1 do wzoru Umowy**.

3. Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w Rozdziale IV.3 pkt 2.1.1 SIWZ, składa na Platformie Zakupowej, podpisany kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności dokument, o którym mowa w Rozdziale IV.4 pkt 1.1 SIWZ, w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 oraz ust. 5 pkt 6 ustawy. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Postanowienia Rozdziału IV.4 pkt 2 SIWZ zdanie pierwsze stosuje się.
4. Jeżeli treść informacji przekazanych przez Wykonawcę w JEDZ odpowiada zakresowi informacji, których Zamawiający wymaga poprzez żądanie dokumentów, w szczególności o których mowa w pkt 2.2, Zamawiający zastrzega sobie prawo do odstąpienia od żądania tych dokumentów od Wykonawcy. W takim przypadku dowodem spełniania przez Wykonawcę warunków udziału w postępowaniu oraz braku podstaw wykluczenia są odpowiednie informacje przekazane przez Wykonawcę lub odpowiednio przez podmioty, na których zdolnościach lub sytuacji Wykonawca polega na zasadach określonych w art. 22a ustawy, w JEDZ.

IV.4. Dokumenty składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej.

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w Rozdziale:
   1.1. IV.3 pkt 2.1.1 SIWZ – składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 oraz ust. 5 pkt 5 i 6 ustawy,
   1.2. IV.3 pkt 2.1.2 – 2.1.4 SIWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
      1.2.1. nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
      1.2.2. nie otwarto jego likwidacji ani nie ogłoszono upadłości.
2. Dokumenty, o których mowa w pkt 1.1 oraz 1.2.2, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w pkt 1.2.1, powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem tego terminu.
3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 1, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Postanowienia pkt 2 stosuje się.

IV.5. Zasady i warunki korzystania przez Wykonawcę ze zdolności lub sytuacji innych podmiotów.

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
3. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający żąda złożenia przez Wykonawcę dokumentów, które określają w szczególności:
   3.1. zakres dostępnych Wykonawcy zasobów innego podmiotu,
   3.2. sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,
   3.3. zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego.
4. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdziale IV.3 pkt 2.1.1 – 2.1.9 SIWZ.

IV.6. Klauzule informacyjne w zakresie danych osobowych.

1. W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.), dalej: „RODO" Zamawiający informuje, że:
   1.1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w toku postępowania jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, al. Jana Pawła II, 00-175 Warszawa. Z Administratorem

można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.

1.2. Administrator wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora, wskazanych w pkt 1.1.

1.3. Pani/Pana dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.

1.4. Odbiorcami Pani/Pana danych osobowych mogą być:

1.4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy,

1.4.2. organy kontrolne,

1.4.3. osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330 j.t.),

1.4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.

1.5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 97 ust. 1 ustawy przechowywane będą przez okres 4 lat od dnia zakończenia niniejszego postępowania. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.

1.6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych.

1.7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

1.8. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, a konsekwencje niepodania określonych danych wynikają z ustawy.

Rozdział V. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Komunikacja między Zamawiającym, a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują wyłącznie za pośrednictwem Platformy Zakupowej, z zachowaniem formy elektronicznej. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się ich datę wczytania do Platformy Zakupowej.
2. Postępowanie prowadzone jest pod numerem referencyjnym sprawy: **DPiZP.2610.27.2019**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.
3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem formy elektronicznej za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji istotnych warunków zamówienia (SIWZ). Wniosek należy przesłać za pośrednictwem Platformy Zakupowej. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Treść pytań (bez ujawnienia źródła) wraz z wyjaśnieniami bądź informacje o dokonaniu modyfikacji SIWZ, Zamawiający przekaże Wykonawcom za pośrednictwem Platformy Zakupowej.
5. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego po upływie terminu jego składania, o którym mowa w pkt 4 lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
6. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SIWZ.
7. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
8. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
   8.1. Pani Bożena Strzelecka, tel.: +48 22 242-03-11 w godz. 9.00 – 15.00.
   8.2. Pan Henryk Żywno, tel.: +48 22 595-00-67 w godz. 9.00 – 15.00.

Rozdział VI. Wymagania dotyczące wadium.

1. Wykonawca zobowiązany jest wnieść wadium w wysokości: **19 000,00 zł** (słownie: dziewiętnaście tysięcy złotych zero groszy).
2. Wadium może być wniesione w:
   2.1. pieniądzu,
   2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
   2.3. gwarancjach bankowych,
   2.4. gwarancjach ubezpieczeniowych,
   2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tj.: Dz. U. z 2018 r., poz. 110 z późn. zm.).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy w Banku Gospodarstwa Krajowego III Oddział w Warszawie numer rachunku - 45 1130 1062 8000 0000 0002 8175, z dopiskiem na przelewie: „wadium w postępowaniu na **„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"**.

4. W przypadku wnoszenia wadium w innej formie niż pieniądz Wykonawca wnosi w formie elektronicznej poprzez wczytanie na Platformie Zakupowej oryginału dokumentu wadialnego tj. opatrzonego kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia (wystawców dokumentu). Wadium powinno być oznaczone w następujący sposób: WADIUM – numer referencyjny i nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.
5. Dokument wadium musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 46 ust. 4a i ust. 5 ustawy.
6. Z treści gwarancji/poręczenia powinno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez Zamawiającego, zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a i ust. 5 ustawy.
7. Oferta Wykonawcy, który nie wniesie wadium lub wniesie je w sposób nieprawidłowy zostanie odrzucona.
8. W przypadku wniesienia wadium i niezłożenia oferty, Wykonawca jest zobowiązany złożyć do Zamawiającego wniosek o zwrot wadium.

Rozdział VII. Termin związania ofertą.

Wykonawcy pozostają związani złożoną ofertą przez 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział VIII Opis sposobu przygotowywania ofert.

VIII.1. Przygotowanie ofert.

1. Ofertę należy złożyć pod rygorem nieważności w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 do SIWZ). Oferta oraz dokumenty, co do których wymagana jest forma oryginału, muszą zostać podpisane indywidualnie (każdy z nich) kwalifikowanym podpisem elektronicznym (każdy plik osobno podpisany kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności).
2. Treść złożonej oferty musi odpowiadać treści niniejszej SIWZ. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, w postaci elektronicznej pod rygorem nieważności i podpisana kwalifikowanym podpisem elektronicznym wyłącznie za pośrednictwem Platformy Zakupowej.
3. Oferta powinna zawierać jedną, jednoznacznie opisaną propozycję.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji określonych w art. 86 ust. 4 ustawy, tj. nazwa (firma) Wykonawcy, adres Wykonawcy, informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji, warunków płatności zawarte w ofercie.

   Uwaga: Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2018 r. poz. 419), które Wykonawca pragnie zastrzec jako tajemnicę przedsiębiorstwa, muszą zostać załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla Informacji stanowiących tajemnicę przedsiębiorstwa.
6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia, w takim przypadku:
   6.1. oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie,
   6.2. każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi udokumentować, że nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12 – 23 oraz art. 24 ust. 5 ustawy, a także złożyć informację lub listę, o której mowa w Rozdziale IV.3 pkt 1 SIWZ,
   6.3. zgodnie z art. 23 ust. 2 ustawy muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia lub do reprezentowania ich w postępowaniu oraz zawarcia umowy o udzielenie przedmiotowego zamówienia publicznego,
   6.4. wszelka korespondencja oraz rozliczenia dokonywane będą wyłącznie z pełnomocnikiem,
   6.5. przed podpisaniem umowy przedłożą pełnomocnictwo do zawarcia umowy w sprawie zamówienia publicznego, jeżeli pełnomocnictwo takie nie zostało dołączone do oferty.

VIII.2. Forma dokumentów składanych w postępowaniu.

1. Wszystkie dokumenty wchodzące w skład oferty oraz składane w trakcie postępowania należy złożyć na Platformie Zakupowej w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579 z późn. zm.).
2. Dokumenty i oświadczenia wchodzące w skład oferty oraz składane w trakcie postępowania, sporządzone w językach obcych muszą być złożone wraz z tłumaczeniami na język polski.
3. Dokumenty lub oświadczenia, o których mowa w Rozporządzeniu w sprawie rodzajów dokumentów, składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem.
4. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.
5. Poświadczenia za zgodność z oryginałem elektronicznej kopii dokumentu lub oświadczenia, o której mowa w pkt 4 następuje przy użyciu kwalifikowanego podpisu elektronicznego.

6. Ilekroć w SIWZ, a także w załącznikach do SIWZ występuje wymóg podpisywania dokumentów lub oświadczeń lub też potwierdzania dokumentów lub oświadczeń za zgodność z oryginałem, należy przez to rozumieć że oświadczenia i dokumenty te powinny być opatrzone kwalifikowanym podpisem elektronicznym osoby (osób) uprawnionej (uprawnionych) do reprezentowania Wykonawcy/podmiotu na zasobach lub sytuacji, którego Wykonawca polega, zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub osobę (osoby) upoważnioną do reprezentowania Wykonawcy/podmiotu na zasobach lub sytuacji, którego Wykonawca polega na podstawie pełnomocnictwa.

Rozdział IX. Miejsce oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty.

IX.1. Miejsce oraz termin składania ofert i otwarcia ofert.

1. Ofertę pod rygorem nieważności należy złożyć w postaci elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Ofertę należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej https: https://platformazakupowa.pl/pn/arimr.
2. Termin składania ofert upływa w dniu **29.10.2019 r. o godzinie 11:00** Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone po upływie terminu przewidzianego na wniesienie odwołania, po uprzednim zawiadomieniu Wykonawcy o fakcie złożenia oferty po terminie.
3. Otwarcie ofert odbędzie się w dniu **29.10.2019 r. o godzinie 11:15** w biurze Zamawiającego, pod adresem ul. Poleczki 33, 02-822 Warszawa.
4. Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SIWZ.

IX.2. Warunki zmiany i wycofania złożonej oferty.

1. Wykonawca posiadający konto na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić lub wycofać ofertę.
2. Wykonawca nie posiadający konta na Platformie Zakupowej, za jej pośrednictwem może przed upływem terminu składania ofert samodzielnie zmienić ofertę. Wykonawca niezalogowany nie może samodzielnie wycofać oferty. W celu wycofania oferty należy skontaktować się z Centrum Wsparcia Klienta uruchomione przez Operatorem Platformy Zakupowej, które służy pomocą techniczną od 7:00 do 17:00 od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mail: cwk@platformazakupowa.pl.
3. Na Platformie Zakupowej w zakładce „Instrukcje dla Wykonawców" opisana jest szczegółowa procedura zmiany i wycofania oferty.
4. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty (załączników).

Rozdział X. Opis sposobu obliczenia ceny.

1. Wykonawca zobowiązany jest do wyliczenia i podania cen jednostkowych, ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 do SIWZ.
2. Ceny określone w Formularzu Ofertowym powinny zawierać wszystkie koszty związane z wykonaniem przedmiotu zamówienia. Podane ceny nie podlegają zmianom przez okres obowiązywania umowy, z zastrzeżeniem postanowień Rozdziału XIV pkt 4 niniejszej SIWZ.
3. Ceny określone w formularzu ofertowym muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (wg zasady zaokrąglenia: poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Wszystkie ceny podane w Formularzu Ofertowym powinny być wyrażone w złotych polskich.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, obowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

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

1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował poniższymi kryteriami:

   1.1. kryterium **cena** (P_c) **– waga 60% [60 pkt],** wg poniższego wzoru

   $$P_C = \frac{C_{min.}}{C_b} \text{ x 60 pkt}$$

   gdzie:
   P_C – ilość punktów oferty badanej w kryterium cena
   $C_{min.}$ – cena najniższa spośród ważnych ofert
   C_b – cena oferty badanej

   1.2. kryterium **„Parametry techniczne Sprzętu IT"** (P_T) **– waga 30% [30 pkt]**, wg poniższych zasad

   W ramach tego kryterium oferta może otrzymać łącznie nie więcej niż 30 pkt. Sumowaniu będą podlegały punkty przyznane badanej ofercie w poszczególnych pozycjach.

   W przypadku gdy zaoferowany Sprzęt IT (poza wymaganiami podstawowymi) będzie posiadał dodatkowo parametry techniczne określone w poniższej tabeli, oferta takiego Wykonawcy otrzyma punkty według poniższej tabeli.

Lp.	„Parametry techniczne Sprzętu IT" (P_T)	**Ilość punktów** *w przypadku zaoferowania Sprzętu IT spełniającego wszystkie parametry techniczne opisane w danej pozycji*
1.	Automatycznie identyfikuje aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną	**3 pkt**
2.	Blokuje transmisję plików szyfrowanych co najmniej: 1. Dokumentów office (doc, xls, ppt, docx, xlsx, pptx) 2. Plików skompresowanych (zip, rar)	**3 pkt**
3.	Wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym/fizycznym	**3 pkt**
4.	Posiada koncept konfiguracji kandydackiej którą można dowolnie edytować na Firewall-u bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji Firewall-a do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym: a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji	**3 pkt**
5.	Sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem do użycia) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w Firewall-a i nie może wymagać korzystania z rozwiązań trzecich	**3 pkt**
6.	W przypadku utraty komunikacji z centralnym systemem zarządzania Firewall musi pozwalać na: 1. Lokalne konfigurowanie reguł bezpieczeństwa 2. Lokalne zbieranie i analizowanie logów 3. Korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym, b. aplikacjach, c. zagrożeniach, d. filtrowaniu stron www. 4. Tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML 5. Tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu	**3 pkt**
7.	System zarządzania, logowania i raportowania posiada taki sam graficzny Interfejs Użytkownika (GUI) jak zarządzane Firewall-e	**3 pkt**
8.	System zarządzania, logowania i raportowania Firewall-ami umożliwia dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek	**3 pkt**
9.	System zarządzania, logowania i raportowania Firewall-i umożliwia zarządzanie posiadanymi przez Zamawiającego urządzeniami Palo Alto Networks PA-5060 w całościowym zakresie opisanym w wymaganiach dla tego systemu	**6 pkt**

Uwagi:

i. *W przypadku nie przekreślenia żadnego ze zwrotów lub łącznego przekreślenia obu zwrotów „TAK/NIE" przez Wykonawcę dla danej pozycji w Formularzu Ofertowym, Zamawiający uzna że zaoferowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.*

ii. *Wykonawca może zaoferować Sprzęt IT spełniający wymagania opisane przez Zamawiającego na wszystkie ww. pozycje (tj. 9 pozycji) lub na dowolnie wybrane przez siebie pozycje. Zamawiający będzie oceniał oferowane parametry techniczne Sprzętu IT dla każdej z pozycji, punkty będą przyznawane adekwatnie do dokonanej oceny oferty.*

1.3. kryterium **„Termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w 4 ust. 1 wzoru Umowy" (P_D) – waga 10% [10 pkt]**, wg poniższych zasad

Lp.	**Termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy** – w Dniach Roboczych.	**Ilość punktów**
1	20 Dni Roboczych	0 pkt
2	19-18 Dni Roboczych	2 pkt
3	17-16 Dni Roboczych	8 pkt
4	15 i mniej Dni Roboczych	10 pkt

Uwagi:

a) *Maksymalny termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy wynosi 20 Dni Roboczych.*

b) *Jeżeli Wykonawca zaoferuje termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy dłuższy niż 20 Dni Roboczych oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z treścią SIWZ.*

c) *W przypadku braku wskazania terminu, o którym mowa powyżej, Zamawiający uzna, że Wykonawca zaoferował maksymalny termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy tj.: 20 Dni Roboczych.*

2. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą liczbę punktów, obliczoną z dokładnością do dwóch miejsc po przecinku, wg wzoru:

$$P = P_c + P_T + P_D$$

gdzie:

P – ilość punktów oferty w łącznym kryterium oceny ofert;
P_c – ilość punktów oferty w kryterium „**Cena**";
P_T – ilość punktów oferty w kryterium „**Parametry techniczne Sprzętu IT**";
P_D – ilość punktów oferty w kryterium **„Termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w 4 ust. 1 wzoru Umowy".**

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

1. Zamawiający powiadomi wybranego Wykonawcę o miejscu i terminie podpisania umowy.
2. Wykonawca będzie zobowiązany do niezwłocznego podania Zamawiającemu danych niezbędnych do sporządzenia umowy lub przekazania dokumentów, które okażą się konieczne do zawarcia umowy.

Rozdział XIII. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

1. Zamawiający żąda od Wykonawcy z którym zostanie podpisana umowa wniesienia zabezpieczenia należytego wykonania umowy w wysokości **10 %** ceny całkowitej podanej w ofercie.
2. Zabezpieczenie należytego wykonania umowy może być wniesione w następujących formach:
   2.1. pieniądzu,
   2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   2.3. gwarancjach bankowych,
   2.4. gwarancjach ubezpieczeniowych,
   2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
3. W przypadku wniesienia zabezpieczenia w formie pieniężnej Zamawiający przechowuje je na oprocentowanym rachunku bankowym.
4. Zabezpieczenie wnoszone w formie gwarancji bankowej, ubezpieczeniowej, poręczenia bankowego lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, poręczenia udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, ma być wystawione przez bank, ubezpieczyciela lub poręczyciela. Bank, ubezpieczyciel, poręczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę zabezpieczenia, na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego jest uzasadnione czy nie.
5. W przypadku, gdy zabezpieczenie, o którym mowa w niniejszym Rozdziale SIWZ będzie wnoszone w formie innej niż pieniądz, Zamawiający zastrzega sobie prawo do akceptacji projektu ww. dokumentów.
6. Zabezpieczenia w innej formie niż pieniądz, Wykonawca złoży u Zamawiającego w Kancelarii Głównej, mieszczącej się w Warszawie przy ul. Poleczki 33, z adnotacją „dla Departamentu Informatyki".
7. Zabezpieczenie należytego wykonania umowy służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
8. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone w terminach i na zasadach określonych we wzorze umowy.

Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego.

1. Zawarcie umowy nastąpi wg wzoru Umowy Zamawiającego, stanowiącego Załącznik nr 6 do niniejszej SIWZ.
2. Postanowienia ustalone we wzorze Umowy nie podlegają negocjacjom.
3. Przyjęcie niniejszych postanowień umowy stanowi jeden z istotnych warunków przyjęcia oferty.
4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Warunki zmian zostały opisane przez Zamawiającego we wzorze Umowy wraz z załącznikami, stanowiącym Załącznik nr 6 do SIWZ.

Rozdział XV. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia publicznego.

1. Wykonawcom, którzy mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w dziale VI ustawy.
2. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie ustawy.
3. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
5. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
   6.1. 10 (dziesięciu) dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej, albo w terminie 15 (piętnastu) dni – jeżeli zostały przesłane w inny sposób;
   6.2. 10 (dziesięciu) dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia SIWZ na stronie internetowej – wobec treści ogłoszenia oraz wobec postanowień SIWZ;
   6.3. 10 (dziesięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia – wobec czynności innych niż określone w pkt 6.1 i 6.2 powyżej.
7. W przypadku wniesienia odwołania wobec treści ogłoszenia o zamówieniu lub postanowień SIWZ Zamawiający może przedłużyć termin składania ofert.
8. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.

Załączniki do SIWZ:

1. Załącznik nr 1 wzór Formularza Ofertowego.
2. Załącznik nr 2 - wzór Oświadczenie o braku podstaw wykluczenia.
3. Załącznik nr 3 - wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej.
4. Załącznik nr 4 - wzór Oświadczenia – Wykaz dostaw (*warunek udziału w postępowaniu*)
5. Załącznik nr 5 - wzór Oświadczenia – Wykaz osób (*warunek udziału w postępowaniu)*.
6. Załącznik nr 6 – wzór Umowy wraz z załącznikami.
7. Załącznik nr 7 - ESPD – plik, w formacie xml, wygenerowany z narzędzia ESPD – do przygotowania Formularza Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ).

ZASTĘPCA PREZESA

Zatwierdzam SIWZ wraz z załącznikami: Warszawa, 23 .09.2019 r. ....Sebastian Jaworski

podpis Zamawiającego

Załącznik nr 1 do SIWZ wzór Formularza Ofertowego

Formularz Ofertowy
DPiZP.2610.27.2019

Ja(my) niżej podpisany(-i) .....

Działając w imieniu i na rzecz .....

.....

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na **„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"**, zgodnie z wymaganiami określonymi w specyfikacji istotnych warunków zamówienia i wzorze Umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia za cenę:

Tabela nr 1A

Firewall'e – 2 szt.

Lp.	Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla pojedynczego Firewall'a	Parametry oferowane (zaznacza Wykonawca)
1	1. Firewall musi być dostarczony jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". 2. Całość Sprzętu IT musi być zarządzana przez jednego producenta.	TAK/NIE*
2	Firewall musi być wyposażony w: 1. 4 interfejsy 100/1000/10GE Ethernet (RJ45) 2. 16 interfejsów 1/10GE SFP+ (z czego 12 interfejsów obsadzonych modułami 10GE SFP+ SR) 3. 4 interfejsy 40GE/100GE QSFP+ lub alternatywnie 4 interfejsy 40GE QSFP+ i 4 interfejsy 100GE QSFP+	TAK/NIE*
3	Firewall musi być wyposażony w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1).	TAK/NIE*
4	Firewall musi być wyposażony w dedykowany port konsoli/zarządzania. Port ten musi być wydzielony logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji.	TAK/NIE*
5	Firewall musi spełniać następujące parametry wydajnościowe, jeżeli Firewall może pracować w różnych trybach to jego wydajność musi być mierzona w trybie pracy, który pozwala na uruchomienie wszystkich wymaganych funkcji Sprzętu IT: 1. minimum 40 Gbps dla Firewall/kontroli aplikacji; 2. minimum 20 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji; 3. minimum 280 tys. nowych połączeń na sekundę; 4. minimum 8 000 000 równoległych sesji.	TAK/NIE*
6	Firewall musi umożliwiać działanie w trzech trybach pracy: 1. rutera (tzn. w warstwie 3 modelu OSI); 2. przełącznika (tzn. w warstwie 2 modelu OSI); 3. w trybie pasywnego nasłuchu (sniffer).	TAK/NIE*
7	Tryb pracy Firewall-a musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).	TAK/NIE*
8	1. Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN. 2. Firewall musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. 3. Firewall musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.	TAK/NIE*

9	1. Firewall musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. 2. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.	TAK/NIE*
10	1. Firewall musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. 2. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). 3. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN	TAK/NIE*
11	1. Firewall musi spełniać następujące parametry wydajnościowe: a) minimum 15Gbps b) minimum 10 000 tuneli IPSEC VPN (site-to-site) c) minimum 15 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. 2. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji lub jeżeli dedykowany klient VPN (dla systemów: Windows, Linux, Android, MacOS) oferowany przez producenta Sprzętu IT wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 15 000 jednoczesnych użytkowników.	TAK/NIE*
12	Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach: 1. Polityki definiujące powinny umożliwiać wykorzystanie: a) adresów źródłowych b) adresów docelowych c) użytkowników d) numerów portów usług e) kategorie URL 2. System musi obsługiwać następujące mechanizmy uwierzytelnienia a) RADIUS lub TACACS+ b) LDAP c) Kerberos lub SAML 2.0	TAK/NIE*
13	Firewall musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie: 1. oznaczania pakietów znacznikami DiffServ; 2. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego; 3. utworzenia 8 klas ruchu sieciowego; 4. kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników; 5. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP; 6. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.	TAK/NIE*
14	Firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP	TAK/NIE*
15	Firewall musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.	TAK/NIE*
16	1. Firewall musi obsługiwać nie mniej niż 50 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. 2. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych).	TAK/NIE*
17	Firewall musi obsługiwać nie mniej niż 25 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 75 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: 1. tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych); 2. Polityk bezpieczeństwa obejmujących: a) System IPS; b) System ochrony antymalware/antyspyware; c) System ochrony antywirus; 3. Koncentratorów VPN dla zdalnego dostępu.	TAK/NIE*

18	Firewall musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.	TAK/NIE*
19	1. Firewall musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie firewall-i. 2. Firewall-e w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.	TAK/NIE*
20	1. Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. 2. Firewall musi umożliwiać zdefiniowanie nie mniej niż 50 000 reguł polityki bezpieczeństwa.	TAK/NIE*
21	1. Identyfikacja aplikacji musi odbywać się poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji Sprzętu IT numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. 2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych. 3. Firewall musi wykrywać 2500 predefiniowanych aplikacji wspieranych przez producenta (w szczególności: Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na Sprzęcie IT bez użycia zewnętrznych narzędzi.	TAK/NIE*
22	1. Firewall musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. 2. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.	TAK/NIE*
23	1. Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. 2. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.	TAK/NIE*
24	1. Firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. 2. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.	TAK/NIE*
25	1. Firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. 2. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.	TAK/NIE*
26	Firewall musi zapewniać ochronę przed atakami typu „Drive-by-download".	TAK/NIE*
27	1. Firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. 2. Wymagana jest obsługa deszyfracji i inspekcji protokołu HTTP/2 zarówno dla ruchu inbound jak i outbound.	TAK/NIE*
28	Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH	TAK/NIE*
29	Firewall musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: 1. Microsoft Active Directory; 2. usługi katalogowe LDAP; 3. serwery Terminal Services.	TAK/NIE*
30	Polityka kontroli dostępu Firewall-a musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.	TAK/NIE*
31	1. Firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. 2. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. 3. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w Firewall który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.	TAK/NIE*
32	1. Firewall musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. 2. System IPS musi działać w warstwie 7 modelu OSI. 3. Baza sygnatur IPS/IDS musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent Sprzętu IT.	TAK/NIE*

	4. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi.	
33	1. Firewall musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. 2. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder, w szczególności: http, smtp, imap, pop3, ftp, smb. 3. Baza sygnatur AV musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń 4. Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. 5. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).	TAK/NIE*
34	1. Firewall musi zapewniać ochronę przed atakami typu Spyware – dopuszcza się by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. 2. Baza sygnatur anty-spyware musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. 3. Reguły/silnik anty-spyware musi być uruchamiany per reguła polityki bezpieczeństwa firewall. 4. Nie jest dopuszczalne, aby funkcja ta była uruchamiana per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi i wsparcia producenta. 6. Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania.	TAK/NIE*
35	1. Firewall musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). 2. Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).	TAK/NIE*
36	Firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	TAK/NIE*
37	1. Firewall musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. 2. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. 3. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. 4. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 6. Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania.	TAK/NIE*
38	1. Firewall musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem. 2. Firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. 3. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to nie wymagane jest jej dostarczenie w chwili zakupu Firewalla/i.	TAK/NIE*
39	1. Zarządzanie Firewall-em musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę www. 2. Dostęp do Firewall-a i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).	TAK/NIE*

40	1. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. 2. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą: a) bazy lokalnej; b) serwera LDAP; c) RADIUS lub TACACS+. 3. Firewall musi zapewniać tworzenie sekwencji uwierzytelniającej posiadającej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).	TAK/NIE*
41	Firewall musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu Firewall-a bez użycia systemu zarządzania lub linii poleceń (CLI).	TAK/NIE*
42	Firewall musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym Firewall-a.	TAK/NIE*
43	Firewall musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.	TAK/NIE*
44	Firewall musi umożliwiać bieżące wysyłanie logów do zewnętrznych serwerów SYSLOG oraz posiadać możliwość wysyłania logów z wykorzystaniem protokołu TCP i zdefiniowana portu docelowego.	TAK/NIE*
45	Firewall musi być wyposażony w zasilacze typu AC pracujące redundantnie.	TAK/NIE*

Uwaga 1

***-niewłaściwe przekreślić.**

Tabela nr 1B

System zarządzania:

Lp.	Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla systemu zarządzania	Parametry oferowane (zaznacza Wykonawca)
1	1. Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania. 2. Dopuszcza się budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta Firewall-i i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. 3. System zarządzania musi pracować w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów.	TAK/NIE**
2	System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMWare.	TAK/NIE**
3	System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne: 1. obsługa nie mniej niż 10 firewalli fizycznych 2. obsługa nie mniej niż 10 firewalli wirtualnych 3. zapewnienie obsługi przestrzeni dyskowej o pojemności nie mniejszej niż 10 TB. 4. Możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczonej na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji)	TAK/NIE**
4	1. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach www. 2. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli	TAK/NIE**

5	System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym: 1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 2. tworzenie statycznych raportów dopasowanych do wymagań Kupującego. 3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 4. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Kupującego z funkcjonalnością „drill-down".	TAK/NIE**
6	System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym: 1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. a) lokalnych (dla wybranych firewalli lub logicznych systemów firewalla). b) globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). 2. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów) 3. pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń. 4. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. 5. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 6. umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.	TAK/NIE**
7	System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym musi: 1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu; 2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli; 3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur; 4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem; 5. pozwalać na zapisywanie różnych wersji konfiguraqi zarządzanych firewalli/logicznych systemów; 6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone; 7. informować o zmianach konfiguracji systemu.	TAK/NIE**
8	System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.	TAK/NIE**

Uwaga 2

**-niewłaściwe przekreślić

TABELA nr 2 – Wymagania dodatkowe punktowane w ramach kryterium „Parametry techniczne Sprzętu IT"

Lp.	„Parametry techniczne Sprzętu IT" (P_T)	Parametr oferowany zaznacza Wykonawca
1.	Automatycznie identyfikuje aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną	TAK/NIE***
2.	Blokuje transmisję plików szyfrowanych co najmniej: 1. Dokumentów office (doc, xls, ppt, docx, xlsx, pptx) 2. Plików skompresowanych (zip, rar)	TAK/NIE ***

3.	Wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym/fizycznym	TAK/NIE ***
4.	Posiada koncept konfiguracji kandydackiej którą można dowolnie edytować na Firewall-u bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji Firewall-a do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym: a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji	TAK/NIE ***
5.	Sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem do użycia) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w Firewall-a i nie może wymagać korzystania z rozwiązań trzecich	TAK/NIE ***
6.	W przypadku utraty komunikacji z centralnym systemem zarządzania Firewall musi pozwalać na: 1. Lokalne konfigurowanie reguł bezpieczeństwa 2. Lokalne zbieranie i analizowanie logów 3. korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym b. aplikacjach c. zagrożeniach d. filtrowaniu stron www 4. tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML 5. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu	TAK/NIE ***
7.	System zarządzania, logowania i raportowania posiada taki sam graficzny Interfejs Użytkownika (GUI) jak zarządzane Firewall-e	TAK/NIE ***
8.	System zarządzania, logowania i raportowania Firewall-ami umożliwia dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek	TAK/NIE ***
9.	System zarządzania, logowania i raportowania Firewall-i umożliwia zarządzanie posiadanymi przez Zamawiającego urządzeniami Palo Alto Networks PA-5060 w całościowym zakresie opisanym w wymaganiach dla tego systemu	TAK/NIE ***

Uwaga 3:

***- **niewłaściwe przekreślić.** *W przypadku nie przekreślenia żadnego ze zwrotów lub łącznego przekreślenia obu zwrotów „TAK/NIE" przez Wykonawcę dla danej pozycji, Zamawiający uzna że zaoferowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.*

TABELA nr 3

Oferujemy Sprzęt IT o parametrach technicznych wymienionych w Tabeli nr 1A i nr 1B oraz w Tabeli nr 2 (punktowane w ramach kryteriów oceny ofert****), oraz na warunkach określonych we wzorze Umowy, który stanowi Załącznik nr 6 do SIWZ **za cenę:**
Uwagi:
**** - *o ile są oferowane*

Lp.	Przedmiot	Cena ofertowa netto zł	Podatek VAT		Cena ofertowa brutto zł
			%	zł	
	a	b	c	d = b x c	e = b + d
1.	Sprzęt IT (Firewall - 2 szt. wraz z systemem zarządzania) oraz z Oprogramowaniem, spełniający wymagania określone w Tabeli nr 1A, nr 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym przez 36 miesięcy wg wymagań zdefiniowanych w § 6 wzoru umowy. ***Producent*** ..... ***Model Firewall***				
2.	Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru Umowy				
Razem [∑1÷2]:			X		

Tabela nr 4

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł) *(cena za 1 godz. konsultacji)*	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1	Konsultacje, o których mowa w § 2 ust. 4 i 5 wzoru Umowy	500 godz.					

Tabela nr 5 - Łączna cena oferty

Przedmiot		Cena netto [zł]	Podatek VAT [zł]	Cena brutto [zł]
[a]	*[b]*	*[c]*	*[d]*	*[e]*
1	Sprzęt IT (Firewall - 2 szt. wraz z systemem zarządzania) oraz z Oprogramowaniem, spełniający wymagania określone w Tabeli nr 1A, nr 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym przez 36 miesięcy wg wymagań zdefiniowanych w § 6 wzoru Umowy oraz Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru umowy, **- wg Tabeli nr 3** *(należy wpisać odpowiednio wartości z Tabeli nr 3 z pozycji „Razem": kol. „b", „d" i „e")*			
2	Konsultacje, o których mowa w § 2 ust. 4 i 5 wzoru Umowy **– wg Tabeli nr 4** *(należy wpisać odpowiednio wartości z Tabeli nr 4: kol. „e", „g" i „h")*			
Łączna cena oferty [∑1÷2]:				

Łączna cena netto oferty ..... zł słownie: _____

Łączna cena brutto oferty ..... zł słownie: _____

Oświadczamy, że:

1. **Termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy wyniesie..... Dni Roboczych.**
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdziale II SIWZ oraz wzorze Umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Zapoznaliśmy się z treścią SIWZ (w tym ze wzorem Umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
5. Uważamy się za związanych niniejszą ofertą na okres wskazany w SIWZ.
6. Wadium w wysokości **19 000,00 zł** (słownie: dziewiętnaście tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
7. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku .....
8. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **10%** ceny całkowitej podanej w ofercie.

9. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.

10. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz firmę Podwykonawcy):

    a) ……

    ……*

* *w* przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*

11. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres: ……

    Dane kontaktowe: imię i nazwisko ……, nr tel. ……, adres e-mail: ……

12. Dokumenty wymienione od strony …… do strony …… stanowią tajemnicę przedsiębiorstwa i nie mogą być ujawnione pozostałym uczestnikom postępowania.

UWAGA:

Zamawiający przypomina, że stosownie do art. 8 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

13. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)* wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**

    ** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1* oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.*).*

    *** w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*

14. Jednocześnie zgodnie z treścią art. 91 ust. 3a ustawy oświadczam, że wybór przedmiotowej oferty:*

    a) **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego

    b) **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług

---

(należy wskazać: nazwę (rodzaj) towarów/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz wartość bez kwoty podatku od towarów i usług)

*) Niepotrzebne skreślić. W przypadku nie skreślenia (nie wskazania) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: *„należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług"* – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

15. Oferta została złożona na _____ stronach kolejno ponumerowanych od nr_____ do nr _____.

Świadom odpowiedzialności karnej oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień złożenia oferty (art. 297 k.k.).

Załącznik nr 2 do SIWZ wzór Oświadczenia o braku podstaw wykluczenia

Dane Wykonawcy
(nazwa; adres)

Oświadczenie o braku podstaw wykluczenia

DPIZP.2610.27.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"** oświadczam(-y), że:

1) nie wydano wobec nas prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne* / wydano wobec nas prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, wobec czego składamy niżej wymienione dokumenty potwierdzające dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności*:
   a) .....,
   b) .....,
   c) .....,
   d) .....,
2) nie wydano orzeczenia wobec nas tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne,
3) niezalegamy z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2018 r. poz. 1445 ze zm.),
4) nie wydano wobec nas prawomocnego wyroku sądu skazującego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym na podstawie art. 24 ust. 5 pkt 5 i 6 ustawy,
5) nie wydano wobec nas ostatecznej decyzji administracyjnej o naruszenie obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym w zakresie określonym na podstawie art. 24 ust. 5 pkt 7 ustawy.

* UWAGA: niepotrzebne skreślić

Załącznik nr 3 do SIWZ wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej

Dane Wykonawcy
(nazwa; adres)

Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej

DPIZP.2610.27.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"**

2) Oświadczamy, że nie należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2019 r., poz. 369)* **z żadnym z Wykonawców, którzy złożyli ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego.

3) Oświadczamy, że należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2019 r., poz. 369)* **z następującymi Wykonawcami, którzy złożyli ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego:

Lp.	Nazwa podmiotu	Siedziba

[*Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia*]

* UWAGA: niepotrzebne skreślić

Załącznik nr 4 do SIWZ wzór Oświadczenia – Wykaz dostaw

[warunek udziału w postępowaniu]

Dane Wykonawcy
(nazwa; adres)

Oświadczenie – Wykaz dostaw
DPIZP.2610.27.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na **„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"**, składamy wykaz dostaw wykonanych (wykonywanych) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, na potwierdzenie spełniania warunku udziału w postępowaniu , o którym mowa w Rozdziale III pkt.1.2.1 SIWZ:

Lp.	Przedmiot wykonanych/wykonywanych dostaw *(wg warunku udziału w postępowaniu: zamówienie polegające na dostawie urządzeń typu Firewall (urządzenia pełniące funkcje zapory ogniowej), wraz z wdrożeniem*	Wartość brutto dostawy w zł *(w przypadku gdy zakres dostawy jest szerszy, należy podać wyłącznie wartość dostawy odpowiadającej treści warunku udziału w postępowaniu w badanym zakresie, wg warunku udziału w postępowaniu: co najmniej **300 000,00 zł brutto**)*	Podmiot na rzecz którego wykonano dostawę *(nazwa i adres)*	Daty wykonania		Dowody	Informacje uzupełniające	
				Od dd-mm-rrrr	Do dd-mm-rrrr		Zasoby innego podmiotu	Nazwa innego podmiotu
1	2	3	4	5	6	7	8	9
1								
2								

Uwaga do kol.7:

1. *Do wykazu należy dołączyć dowody potwierdzające, że powyższe dostawy zostały wykonane lub są wykonywane należycie, tj.:*
   - *1.1. referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane należycie,*
   - *1.2. oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym mowa wyżej w pkt 1.1;*
2. *Należy wpisać nazwę dowodu (dokumentu) potwierdzającego, że dostawy zostały wykonane wykonywane należycie (podać numer strony w ofercie);*

Uwaga do kol.8:

1. *Zaznaczyć „TAK", tylko w przypadku gdy Wykonawca polega na zasobach innego podmiotu dla wykazania spełniania warunku udziału;*
2. *Dla wykazania spełniania warunku udziału w postępowaniu, opisanego w Rozdziale III pkt 1.2.1 SIWZ, Wykonawca może polegać, na zasadach określonych w art.22a ustawy. W tym celu Wykonawca składa dokumenty i oświadczenia zgodnie z zasadami określonymi w Rozdziale IV.5 SIWZ.*

Załącznik nr 5 do SIWZ wzór Oświadczenia — Wykaz osób
[warunek udziału w postępowaniu]

Dane Wykonawcy
(nazwa; adres)

Oświadczenie – Wykaz osób
które będą uczestniczyć w wykonywaniu zamówienia
DPiZP.2610.27.2019

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami**”,” składamy wykaz osób w celu potwierdzenia spełniania warunku udziału w postępowaniu, o którym mowa w **Rozdziale** III pkt 1.2.2 SIWZ, skierowanych przez Wykonawcę do realizacji zamówienia, które będą uczestniczyć w jego wykonaniu:

1. Jedna osoba spełniająca poniższe wymagania:

Wymagania Zamawiającego wskazane w SIWZ	**Wypełnia Wykonawca**					
Osoba, która posiada: 1. co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.2.1. SIWZ z wyłączeniem wartości zamówień; 2. certyfikat Cisco Certified Internetwork Expert (CCIE) Security lub równoważny. *Uwaga:* *Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:* *1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:* *i. analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,* *ii. analogiczny stopień poziomu kompetencji,* *iii. analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,* *2) potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowy certyfikaty muszą być potwierdzone egzaminem).*	1	1.1	Imię i Nazwisko			
		1.2.	Wskazana osoba spełnia wymagania zdefiniowane w Rozdziale III pkt 1.2.2.SIWZ			
		1.3	Posiadany certyfikat	1.3.1	Nazwa certyfikatu	
				1.3.2	Podmiot wydający certyfikat	
				1.3.3	Nr certyfikatu *[o ile dotyczy]*	
				1.3.4	Data ważności certyfikatu [DD-MM-RRRR] *[o ile dotyczy]*	
		1.4		1.4.1	Dysponowanie bezpośrednie	

			Podstawa dysponowania osobą	1.4.2	Dysponowanie osobą na podstawie art. 22a ustawy – Prawo zamówień publicznych	

Uwaga:

1. *Dla wykazania spełniania warunku udziału w postępowaniu opisanego w Rozdziale III pkt 1.2.2. SIWZ, Wykonawca może polegać, na zasadach określonych w art. 22a ustawy, na osobach zdolnych do wykonania zamówienia oddanych mu do dyspozycji przez inne podmioty.*
2. *W odniesieniu do podstawy dysponowania osobą Wykonawca wypełnia kolumnę „Dysponowanie bezpośrednie" albo „Dysponowanie osobą na podstawie art., 22a ustawy – Prawo zamówień publicznych".*
3. *W przypadku dysponowania przez Wykonawcę osobą na podstawie art. 22a ustawy – Prawo zamówień publicznych jest obowiązany udowodnić Zamawiającemu, iż będzie dysponował niezbędnymi osobami zdolnymi do wykonania zamówienia, w szczególności przedstawiając w tym celu dokumenty i oświadczenia w zakresie wskazanym w Rozdziale IV.5 SIWZ.*

Załącznik nr 6 do SIWZ wzór Umowy

Umowa nr ____/DI/2019/2610

zawarta w dniu _____ _____ 2019 r. w Warszawie pomiędzy:

Agencją Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy al. Jana Pawła II nr 70, 00-175 Warszawa, (adres do korespondencji: ARiMR Departament Informatyki ul. Poleczki 33, 02-822 Warszawa), REGON nr 010613083, zarejestrowanym podatnikiem podatku od towarów i usług, NIP 526-19-33-940, zwaną dalej "**Kupującym**" lub „**ARiMR**", którą reprezentuje:

_____ – Zastępca Prezesa ARiMR, Pełnomocnik;
_____ – Dyrektor Departamentu Księgowości, w ramach zajmowanego stanowiska wykonująca obowiązki Głównego Księgowego, Pełnomocnik;

a

_____
_____, zwaną dalej "**Sprzedawcą**", którą reprezentuje:

_____ – _____;
_____ – _____;

zwanych łącznie „**Stronami**".

W wyniku wyboru oferty w postępowaniu o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego zgodnie z art. 39 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 ze zm.), zawarto umowę o następującej treści:

§ 1. Definicje

W niniejszej umowie następujące wyrażenia i określenia będą miały znaczenie zgodnie z podanymi poniżej definicjami, zapisane z dużej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:

1) **Strony** – Sprzedawca i Kupujący wymienieni w komparycji Umowy;
2) **Umowa** – niniejsza umowa wraz z załącznikami regulująca prawa i obowiązki Stron z niej wynikające i związane z jej wykonaniem;
3) **Sprzęt IT** – urządzenia informatyczne, pełniące funkcje ściany ogniowej (firewall)– 2 szt. wraz z systemem zarządzania oraz Oprogramowaniem niezbędnym do zachowania wyspecyfikowanej funkcjonalności Sprzętu IT, szczegółowo opisane w Załączniku nr 1 i 7 do Umowy;
4) **Oprogramowanie** – programy komputerowe dostarczone przez Sprzedawcę, z których Kupujący korzysta na podstawie Licencji udzielonych przez producenta, niezbędne do korzystania ze Sprzętu IT;
5) **Licencja** – prawo do bezterminowego korzystania z Oprogramowania, zgodnie z warunkami określonymi przez producenta Oprogramowania, potwierdzone dokumentem licencyjnym;
6) **Serwis gwarancyjny** – usługa opieki serwisowej i wsparcia technicznego dla Sprzętu IT oraz Oprogramowania, świadczona w zakresie i na zasadach określonych w Umowie oraz zgodnie z warunkami określonymi przez producenta Sprzętu IT i Oprogramowania;
7) **Wdrożenie** – czynności wykonywane przez Sprzedawcę, mające na celu uruchomienie dostarczonego Sprzętu IT, instalację Oprogramowania oraz przeniesienie konfiguracji z dotychczas użytkowanych urządzeń na Sprzęt IT – szczegółowo opisane w Załączniku nr 1 do Umowy;
8) **Dokumentacja powykonawcza** - dokumentacja zawierająca schemat fizyczny i logiczny podłączenia Sprzętu IT, konfigurację Sprzętu IT oraz opis zastosowanych rozwiązań i technologii;
9) **Dokumenty** - instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania;
10) **COPD** – Centralne Ośrodki Przetwarzania Danych Kupującego znajdujące się w Piasecznie ul. Jana Pawła II 66, 05-500 Piaseczno oraz w Warszawie, ul. Poleczki 23, 02-822 Warszawa;
11) **Dni Robocze** – dni w godzinach pracy Kupującego od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych od pracy u Kupującego, o których Kupujący powiadomi Sprzedawcę.

§ 2. Przedmiot Umowy

1. Na podstawie Umowy Sprzedawca:
   1) sprzedaje i dostarczy fabrycznie nowy, nieoszący śladów uprzedniego używania Sprzęt IT wraz z Oprogramowaniem, zgodnie ze specyfikacją stanowiącą Załącznik nr 1 do Umowy oraz z Formularzem ofertowym, stanowiącym Załącznik nr 7 do Umowy;
   2) wykona Wdrożenie;
   3) świadczył będzie Serwis gwarancyjny dla Sprzętu IT i Oprogramowania przez okres 36 miesięcy;

   a Kupujący kupuje Sprzęt IT i Oprogramowanie.

2. Wraz z dostawą Sprzętu IT wraz z Oprogramowaniem Sprzedawca dostarczy Kupującemu Dokumenty.
3. W ramach realizacji Umowy Sprzedawca wykona Dokumentację powykonawczą i dostarczy ją Kupującemu w formie papierowej i elektronicznej do akceptacji i odbioru.
4. W ramach Umowy Sprzedawca zapewni Kupującemu 500 godzin konsultacji technicznych w okresie trwania Serwisu gwarancyjnego. Konsultacje będą obejmowały analizy, audyty oraz rekomendację dot. Sprzętu IT lub Oprogramowania, jak również wszelkiego rodzaju prace rekonfiguracyjne Sprzętu IT lub Oprogramowania oraz pomoc przy pracach technicznych przeprowadzanych przez Kupującego w COPD. Konsultacje będą świadczone w języku polskim. Kupujący zastrzega sobie prawo niewykorzystania pełnej ilości godzin konsultacji. Sprzedawcy z tytułu nie wykorzystania pełnej ilości godzin konsultacji nie przysługują żadne roszczenia odszkodowawcze.
5. W ramach konsultacji technicznych Sprzedawca na wniosek Kupującego przeprowadzi warsztaty lub prezentacje dot. wskazanego elementu Sprzętu IT oraz Oprogramowania w Centrali Kupującego przy ul. Poleczki 33 w Warszawie. Czas dojazdu do Sprzedawcy nie będzie wliczony jako wykorzystanie dostępnej puli godzin.
6. Sprzedawca będzie przyjmował zgłoszenia konsultacyjne od poniedziałku do piątku, w godzinach od 9.00 do 15.00, telefonicznie pod numerem: _____ lub na adres poczty elektronicznej _____@_____. Przyjęcie zgłoszenia zostanie przez Sprzedawcę potwierdzone (drogą elektroniczną na adresy e-mail pracowników Kupującego, wskazanych w § 3 ust. 2 pkt 1 Umowy) w ciągu 1 godziny od otrzymania zgłoszenia. Niepotwierdzenie zgłoszenia w powyższym terminie Kupujący uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu lub numeru telefonu wskazanego powyżej, Sprzedawca zobowiązany jest niezwłocznie powiadomić na piśmie Kupującego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy w formie pisemnego aneksu, a jedynie poinformowania drugiej Strony o zmianie.
7. Na koniec każdego kwartału Sprzedawca przedstawi Protokół odbioru konsultacji ze zgłoszonych i przeprowadzonych konsultacji, którego wzór został określony w Załączniku nr 4b do Umowy.

§ 3. Wymagania dotyczące wykonania Umowy

1. Sprzedawca oświadcza, że posiada konieczne doświadczenie i profesjonalne kwalifikacje niezbędne do prawidłowego wykonania Umowy i zobowiązuje się do wykonania Umowy przy zachowaniu należytej staranności określonej w art. 355 § 2 Kodeksu Cywilnego.
2. Osobami upoważnionymi do rozpatrywania bieżących spraw i podpisywania protokołów odbioru związanych z wykonaniem Umowy, przy zachowaniu określonych w niej warunków, w tym terminów:
   1) po stronie Kupującego są:
      Pan _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
      Pan _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
      Pan _____ tel.: (22) _____; e-mail: _____@arimr.gov.pl
   2) po stronie Sprzedawcy są:
      Pan/i _____ tel.: (XX) _____; e-mail: _____@_____
      Pan/i _____ tel.: (XX) _____; e-mail: _____@_____
3. Zmiana osób, o których mowa w ust. 2 powyżej, nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.
4. Sprzedawca oświadcza, że Sprzęt IT posiada wszelkie certyfikaty i homologacje niezbędne do eksploatacji na terytorium Rzeczypospolitej Polskiej oraz gwarantuje, że Sprzęt IT jest zgodny z Polskimi Normami niezawodności i bezpieczeństwa.
5. Kupujący wymaga a Sprzedawca oświadcza, że Wdrożenie będzie wykonywane bezpośrednio przez minimum 1 osobę posiadającą uprawnienia CCIE Security lub równoważne. W ramach Wdrożenia wymagane będzie przeniesienie funkcjonalności z dwóch urządzeń PA5060. Wykaz osób (zgodny ze złożonym w postępowaniu) stanowi Załącznik nr 8 do Umowy. Wykonawca może dokonać zmiany osoby wskazanej w Wykazie osób na inną osobę posiadającą specjalistyczne kwalifikacje, o których mowa w niniejszym punkcie, potwierdzone odpowiednimi certyfikatami, po uprzednim pisemnym powiadomieniu i uzyskaniu akceptacji Zamawiającego. Zmiana osoby, o której mowa w zdaniu poprzedzającym nie wymaga formy aneksu. W przypadku zmiany osoby wskazanej w Wykazie osób, nowa osoba musi posiadać kwalifikacje i doświadczenie nie gorsze od osoby wskazanej w wykazie osób złożonym wraz z ofertą.
6. W terminie do 3 Dni Roboczych po podpisaniu przez upoważnionych przedstawicieli Stron Umowy, Kupujący przekaże Sprzedawcy aktualną konfigurację urządzeń, o których mowa w ust. 5 oraz zapisy konfiguracji do przeniesienia z urządzeń PA5060 pracujących w sieci LAN Kupującego.

§ 4. Terminy i odbiory

1. Dostarczenie Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenie nastąpi w lokalizacjach COPD nie później niż w terminie do ___ *(zostanie uzupełnione zgodnie z ofertą Wykonawcy)* Dni Roboczych od dnia zawarcia Umowy.
2. Sprzedawca powiadomi, w formie pisemnej, Kupującego o terminie dostarczenia Sprzętu IT wraz z Oprogramowaniem, i Dokumentów oraz o terminie rozpoczęcia Wdrożenia w poszczególnych lokalizacjach COPD, z wyprzedzeniem co najmniej 5 Dni Roboczych. W terminie do 2 Dni Roboczych Kupujący potwierdzi wskazany termin lub wskaże inny, jednak nie później niż 2 Dni Robocze od daty otrzymania przez Kupującego ww. powiadomienia.
3. Dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentów odbędzie się na koszt i ryzyko Sprzedawcy. Sprzedawca dostarczy Sprzęt IT wraz z Oprogramowaniem i Dokumenty zgodnie z warunkami Umowy i poniesie pełne ryzyko związane z niebezpieczeństwem utraty albo uszkodzenia Sprzętu IT wraz z Oprogramowaniem do dokonania ich odbioru przez osobę upoważnioną przez Kupującego, zgodnie z ust. 4 - 10.

4. Odbiór Sprzętu IT wraz z Oprogramowaniem i Dokumentów zostanie dokonany komisyjnie z udziałem upoważnionych przedstawicieli Sprzedawcy i Kupującego. Odbiór i zawiadomienia Stron dotyczące odbioru i Wdrożenia będą dokonywane w Dniach Roboczych.
5. Podczas odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca w obecności Kupującego:
   1) rozpakuje dostarczony Sprzęt IT oraz sprawdzi czy nie nosi znamion uszkodzeń mechanicznych oraz czy jest fabrycznie nowy i zgodny z Załącznikiem nr 1 i nr 7 do Umowy;
   2) podłączy Sprzęt IT do sieci zasilającej i zainstaluje Oprogramowanie;
   3) usunie z miejsca dostarczenia i zutylizuje wszelkie opakowania, pozostałe po dostarczeniu i zainstalowaniu Sprzętu IT;
   4) wykona Wdrożenie, zgodnie z ust. 6.
6. W ramach Wdrożenia Sprzedawca w obecności pracownika Kupującego:
   1) przygotuje konfigurację dostarczanego Sprzęt IT (konfiguracja podstawowa – adresacja IP, konfiguracja klastra rozciągniętego na dwie lokalizacje);
   2) przeniesie listy kontroli dostępu z urządzeń PA5060 i z przełączników Kupującego oraz wdroży je na Sprzęcie IT, z uwzględnieniem funkcjonalności grup obiektowych;
   3) zainstaluje Sprzęt IT i skonfiguruje Oprogramowanie w lokalizacjach COPD (adresacja IP, ustawienie dostępu do dostarczonego Sprzętu IT, utworzenie i konfiguracja kont użytkowników);
   4) uruchomi Sprzęt IT produkcyjnie z pełnymi funkcjonalnościami przeniesionymi z urządzeń PA5060.
7. Po dokonaniu przez Kupującego bez zastrzeżeń odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz Wdrożenia w ostatniej lokalizacji COPD, Kupujący podpisze Protokół odbioru, którego wzór stanowi Załącznik nr 2 do Umowy.
8. W przypadku stwierdzenia podczas odbioru, że:
   1) Sprzęt IT lub Oprogramowanie są niezgodne z Załącznikiem nr 1 lub Załącznikiem nr 7 do Umowy lub posiadają ślady zewnętrznego uszkodzenia lub
   2) nie dostarczono wszystkich wymaganych Dokumentów, o których mowa w ust. 1 lub
   3) Wdrożenie nie zostało wykonane prawidłowo lub
   4) Sprzęt IT wraz z Oprogramowaniem, Dokumenty lub Wdrożenie budzą inne zastrzeżenia niż określone w pkt 1-3,

   Kupujący odmówi podpisania Protokołu odbioru, jednocześnie przekaże Sprzedawcy protokół przedstawiający powód odmowy odbioru ze wskazaniem terminu dostarczenia Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia. Procedura czynności odbioru zostanie przeprowadzona ponownie.
9. W przypadku stwierdzenia podczas powtórnej procedury czynności odbioru którejkolwiek z okoliczności wskazanych w ust. 8, Kupujący odmówi odbioru przedmiotu Umowy i jednocześnie przekaże Sprzedawcy protokół przedstawiający powód odmowy odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów wraz z Wdrożeniem. W sytuacji odmowy odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentów Sprzedawca ma obowiązek odbioru dostarczonego Sprzętu IT wraz z Oprogramowaniem Dokumentów z miejsca dostarczenia w terminie 5 Dni Roboczych od daty przekazania Sprzedawcy protokołu przedstawiającego powody odmowy odbioru Sprzętu IT.
10. W terminie do 5 Dni Roboczych od dnia podpisania Protokołu odbioru, o którym mowa w ust. 7, Sprzedawca dostarczy do Kupującego Dokumentację powykonawczą. Odbiór zostanie potwierdzony Protokołem odbioru Dokumentacji powykonawczej, którego wzór stanowi Załącznik nr 3. Kupujący zastrzega sobie prawo zgłaszania uwag do Dokumentacji powykonawczej. Sprzedawca zobowiązany jest uwzględnić uwagi Kupującego lub zgłosić zastrzeżenia w terminie 3 Dni Roboczych od dnia otrzymania uwag od Kupującego.
11. Wszystkie powiadomienia dotyczące odbiorów Sprzętu IT wraz z Oprogramowaniem, Dokumentów, Dokumentacji powykonawczej lub wykonania Wdrożenia powinny być dokonywane w Dni Robocze.

§ 5. Udzielenie Licencji

1. Kupujący, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy, nabywa Licencję upoważniającą do bezterminowego korzystania z Oprogramowania w celu zachowania funkcjonalności Sprzętu IT.
2. Kupujący, w ramach udzielonej Licencji, zgodnie z warunkami producenta Oprogramowania, ma prawo do trwałego lub czasowego zwielokrotnienia Oprogramowania w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym jest to niezbędne dla wprowadzania, wyświetlania, stosowania, przekazywania, przechowywania Oprogramowania dla własnych potrzeb Kupującego, z uwzględnieniem treści ust. 3, zgodnie z jego charakterem i przeznaczeniem, Dokumentami i warunkami Umowy.
3. Licencja uzyskana zgodnie z zapisami ust. 2, może być wykorzystywana wyłącznie dla celów działalności Kupującego i nie obejmuje prawa do wprowadzania Oprogramowania do obrotu lub przekazywania ani w części ani w całości osobom trzecim zarówno odpłatnie, jak i nieodpłatnie w żadnej formie prawnej.
4. W ramach udzielonej Licencji Kupujący jest upoważniony do korzystania z Dokumentów dostarczonych z Oprogramowaniem, na polach eksploatacji wskazanych w ust. 2.

§ 6. Serwis gwarancyjny

1. Serwis gwarancyjny świadczony będzie przez Sprzedawcę przez okres 36 miesięcy od dnia podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy.
2. Sprzedawca zobowiązuje się, że podczas trwania Serwisu gwarancyjnego, po otrzymaniu zgłoszenia serwisowego od Kupującego, na własny koszt i ryzyko, naprawi lub wymieni w terminach określonych w niniejszym paragrafie wadliwy Sprzęt IT na wolny od wad oraz usunie skutki tych wad. Naprawy będą dokonywane bezpośrednio przez Sprzedawcę w lokalizacji COPD, w której dokonano Wdrożenia Sprzętu IT, którego dotyczy wada.
3. Serwis gwarancyjny obejmuje dokonanie naprawy, w tym wymianę podzespołów na nowe, a także dojazd serwisanta,

transport Sprzętu IT oraz podstawienie urządzeń zastępczych.

4. W ramach Serwisu gwarancyjnego Sprzedawca dokona naprawy Sprzętu IT najpóźniej w ciągu 6 godzin od otrzymania zgłoszenia serwisowego, o którym mowa w ust. 2, przy czym naprawa Sprzętu IT powinna być dokonana przez serwisanta posiadającego właściwe kwalifikacje techniczne.
5. Sprzedawca, w przypadku niemożności dokonania naprawy w terminie wskazanym w ust. 4, zobowiązany jest dokonać w tym terminie wymiany wadliwego Sprzętu IT na fabrycznie nowy, wolny od wad. Obowiązek, o którym mowa w zdaniu poprzednim dotyczy również sytuacji, gdy wada, usterka lub inna nieprawidłowość Sprzętu IT nie zostanie usunięta w wyniku dokonania naprawy po raz trzeci, przy czym termin na dostarczenie Sprzętu IT w takim wypadku wynosi 12 godzin od otrzymania przez Sprzedawcę czwartego zgłoszenia serwisowego dotyczącego tego samego Sprzętu IT. W przypadku, gdy dostarczenie takiego samego Sprzętu IT nie będzie możliwe, Sprzedawca dostarczy nowy Sprzęt IT o parametrach technicznych nie gorszych od określonych w Załączniku nr 1 i 7 do Umowy. Dostarczenie zastępcze wymaga zgody Kupującego.
6. Sprzedawca będzie przyjmował zgłoszenia serwisowe Kupującego od osób wskazanych pisemnie przez Kupującego, w trybie 24 godziny na dobę 7 dni w tygodniu (tryb 24/7) telefonicznie pod numerem: (XX) _____, faksem pod numerem (XX) _____ lub na adres poczty elektronicznej: _____@_____ Przyjęcie zgłoszenia zostanie przez Sprzedawcę potwierdzone (drogą elektroniczną na wskazany przez Kupującego adres e-mail) w ciągu 1 godziny od otrzymania zgłoszenia. Niepotwierdzenie zgłoszenia w powyższym terminie Kupujący uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu lub numerów telefonów i faksów wskazanych powyżej, Sprzedawca zobowiązany jest niezwłocznie powiadomić na piśmie Kupującego. Zmiana danych, o których mowa w zdaniu poprzedzającym nie wymaga zmiany Umowy. Usunięcie wady lub wymiana Sprzętu IT zostaną potwierdzone Protokołem odbioru usunięcia wady podpisanym przez upoważnionych przedstawicieli Stron, sporządzonym według wzoru stanowiącego Załącznik nr 4a do Umowy.
7. Dla Sprzętu IT przez naprawę należy rozumieć przywrócenie takiego stanu, w którym Sprzęt IT pracuje poprawnie i spełnia wszystkie funkcjonalności określone w Załączniku nr 1 i 7 do Umowy.
8. Wszelkie koszty związane ze świadczeniem Serwisu gwarancyjnego obciążają Sprzedawcę.
9. Niezależnie od uprawnień z tytułu Serwisu gwarancyjnego (gwarancji) Kupującemu przysługują wobec Sprzedawcy uprawnienia z tytułu rękojmi. Jeżeli w ramach rękojmi Kupujący zażąda wykonania przez Sprzedawcę obowiązków, określonych w niniejszym paragrafie, do terminów realizacji poszczególnych obowiązków z tytułu rękojmi mają odpowiednie zastosowanie terminy określone dla tych obowiązków w ust. 4 lub 5.
10. Kupujący zastrzega sobie prawo do zmiany lokalizacji COPD (w obrębie Warszawy). Kupujący odinstaluje, przewiezie, dokona instalacji i uruchomi Sprzęt IT w nowej lokalizacji COPD. Uruchomienie Sprzętu IT odbędzie się w asyście przedstawiciela Sprzedawcy, jeśli Sprzedawca poinformuje Kupującego o zamiarze uczestniczenia w uruchomieniu Sprzętu IT w nowej lokalizacji COPD. Nieobecność przedstawiciela Sprzedawcy podczas uruchomienia Sprzętu IT w nowej lokalizacji nie wpływa na uruchomienie przez Kupującego Sprzętu IT oraz nie zwalnia Sprzedawcy z obowiązku świadczenia zobowiązań wynikających z Umowy zgodnie z jej postanowieniami. Zmiana lokalizacji COPD nie wymaga zmiany Umowy w formie pisemnego aneksu a jedynie poinformowania osób wskazanych przez Sprzedawcę w § 3 ust. 2 Umowy o takiej zmianie na 5 Dni Roboczych przed planowaną zmianą lokalizacji COPD. Od momentu przekazania informacji o uruchomieniu Sprzętu IT w nowej lokalizacji COPD, Sprzedawca świadczyć będzie zobowiązania wynikające z Umowy dla zmienionej lokalizacji COPD.
11. W ramach Serwisu gwarancyjnego Kupujący będzie miał prawo dostępu do serwisu producenta Oprogramowania, w tym do:
    1) aktualizacji wersji Oprogramowania (*updates, upgrade, patches*) oraz nowych wersji Oprogramowania i udoskonaleń do wersji bieżących Oprogramowania (nowych edycji Oprogramowania, wydań uzupełniających, poprawek programistycznych); Kupujący, w ramach wynagrodzenia, uzyskuje prawo do zainstalowania, uruchamiania, przechowywania i nieograniczonego w czasie korzystania z aktualizacji,
    2) monitorowania statusu zgłoszeń serwisowych;
    3) samodzielnego oraz za pośrednictwem Sprzedawcy zgłaszania awarii do producenta;
    4) samodzielnego oraz za pośrednictwem Sprzedawcy dostępu do bazy Oprogramowania, bazy wiedzy, dokumentacji i forum dyskusyjnego producenta Sprzętu IT, o ile takie istnieją;
    5) dostępu do bazy Oprogramowania, bazy wiedzy, dokumentacji i forum dyskusyjnego producenta, o ile takie istnieje.

§ 7. Wynagrodzenie

1. Łączne wynagrodzenie z tytułu wykonania Umowy wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100), z czego:
    1) wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem oraz Serwis gwarancyjny wynosi netto ..... zł (słownie złotych ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100),
    2) wynagrodzenie za Wdrożenie i Dokumentację powykonawczą wynosi netto ..... zł (słownie złotych: ..... XX/100), powiększone o należny VAT co daje kwotę brutto ..... zł (słownie złotych: ..... XX/100),
    3) maksymalne wynagrodzenie z tytułu konsultacji, o których mowa w § 2 ust. 4 Umowy wynosi netto _____,XX zł (słownie złotych: _____ XX/100) powiększone o należny podatek od towarów i usług, co daje kwotę brutto _____,XX zł (słownie złotych: _____ XX/100).
2. Wynagrodzenie, o którym mowa w:

1) ust. 1 pkt 1-2 płatne będzie na podstawie faktury VAT wystawionej przez Sprzedawcę, w terminie do 28 dni licząc od dnia otrzymania przez Kupującego prawidłowo wystawionej faktury VAT łącznie z podpisanym bez zastrzeżeń przez upoważnionych przedstawicieli Stron Protokołem odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy, stanowiącym podstawę wystawienia faktury VAT;
2) w ust. 1 pkt 3 płatne będzie każdorazowo w terminie do 28 dni licząc od daty otrzymania przez Kupującego prawidłowo wystawionej faktury oraz podpisanego bez zastrzeżeń przez upoważnionych przedstawicieli Stron protokołu konsultacji o którym mowa w § 2 ust. 7 Umowy. Wynagrodzenie o którym mowa w zdaniu poprzednim (za konsultacje), rozliczane jest kwartalnie i wyliczane jako iloczyn ilości godzin konsultacji odebranych w danym kwartale i ceny za jedną godzinę konsultacji określoną zgodnie z ofertą Sprzedawcy na kwotę netto _____,XX zł (słownie złotych: _____ _____ XX/100) powiększoną o należny podatek VAT.

3. Wynagrodzenie, o którym mowa w ust. 1, wyczerpuje wszelkie roszczenia finansowe Sprzedawcy z tytułu wykonania Umowy, w tym uwzględnia konsultacje, o których mowa w § 2 ust. 4 Umowy.
4. Za termin wykonania płatności uznaje się dzień obciążenia rachunku bankowego Kupującego.
5. Błędnie wystawiona faktura VAT lub brak podpisanego przez umocowanych przedstawicieli Stron Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy spowodują naliczenie ponownego, 28-dniowego terminu płatności od dostarczenia prawidłowo wystawionej faktury VAT lub podpisanego Protokołu odbioru Dokumentacji powykonawczej.
6. Błędnie wystawiona faktura VAT lub brak podpisanego przez umocowanych przedstawicieli Stron Protokołu odbioru konsultacji, o którym mowa w § 2 ust. 7 Umowy spowodują naliczenie ponownego, 28-dniowego terminu płatności od dostarczenia prawidłowo wystawionej faktury VAT lub Protokołu odbioru konsultacji.
7. Jeżeli w trakcie realizacji Umowy nastąpi:
   1) zmiana stawki podatku od towarów i usług,
   2) zmiana wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. z 2018, poz. 2177 tj.),
   3) zmiana zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,
   4) zmiana zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych,

   a zmiany te będą miały wpływ na koszty wykonania Umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Sprzedawcy określone w ust. 8-15 poniżej.
8. Zmiana wysokości wynagrodzenia wymaga zmiany Umowy w drodze aneksu.
9. Sprzedawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany o których mowa w ust. 7 uprawniony jest do wystąpienia do Kupującego z pisemnym wnioskiem o dokonanie zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez Kupującego, czy zmiany, o których mowa w ust. 7, mają wpływ na koszty wykonania Umowy przez Sprzedawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Sprzedawcy określonego w niniejszej Umowie, a w szczególności:
   1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Sprzedawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Sprzedawcę.
   2) przyjęte przez Sprzedawcę zasady kalkulacji wysokości kosztów wykonania Umowy oraz założenia co do wysokości dotychczasowych oraz przyszłych kosztów wykonania Umowy, wraz z dokumentami potwierdzającymi prawidłowość przyjętych założeń - takimi jak np. umowy o pracę, dokumenty potwierdzające zgłoszenie pracowników do ubezpieczeń.
10. W terminie 30 dni od otrzymania wniosku o którym mowa w ust. 9, Kupujący może zwrócić się do Sprzedawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).
11. Kupujący w terminie 30 dni od dnia otrzymania kompletnego wniosku zajmie w stosunku do niego pisemne stanowisko. Za dzień przekazania stanowiska uznaje się dzień jego wysłania na adres właściwy dla doręczeń pism dla Sprzedawcy.
12. Kupujący najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 7 może przekazać Sprzedawcy pisemny wniosek o dokonanie zmiany Umowy. Wniosek powinien zawierać co najmniej propozycję zmiany Umowy w zakresie wysokości wynagrodzenia oraz powołanie zmian przepisów.
13. Przed przekazaniem wniosku, o którym mowa w ust. 12, Kupujący może zwrócić się do Sprzedawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez Kupującego, czy zmiany, o których mowa w ust. 7, mają wpływ na koszty wykonania Umowy przez Sprzedawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi Kupujący. Postanowienia ust. 10-15 stosuje się odpowiednio, z tym, że Sprzedawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od Kupującego.
14. W przypadku niewykonania lub nienależytego wykonania przez Sprzedawcę zobowiązania określonego w ust. 13 w terminie określonym w ust. 13, Sprzedawca zapłaci na rzecz Kupującego karę umowną w wysokości 0,1 % wynagrodzenia brutto określonego w ust.1 za każdy rozpoczęty dzień kalendarzowy opóźnienia. Jeżeli w terminie określonym w ust. 13 Sprzedawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 13 lub przedłożone przez Sprzedawcę wyjaśnienia lub dokumenty będą niewystarczające do dokonania przez Kupującego oceny, o której mowa w ust. 13 – Kupujący wyznaczy Sprzedawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub

uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, Kupujący uprawniony będzie do wypowiedzenia Umowy z zachowaniem miesięcznego terminu wypowiedzenia.

15. Jeżeli w trakcie procedury opisanej w ust. 9-14 zostanie wykazane, że zmiany, o których mowa w ust. 7 uzasadniają zmianę wysokości wynagrodzenia, Strony uzgodnią treść aneksu do Umowy oraz podpiszą aneks, z zachowaniem zasady zmiany wysokości wynagrodzenia w kwocie odpowiadającej zmianie kosztów wykonania Umowy wywołanych przyczynami określonymi w ust. 7.

§ 8. Kary umowne i roszczenia odszkodowawcze

1. W przypadku opóźnienia Sprzedawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz w realizacji Wdrożenia w terminie wskazanym w § 4 ust. 1 lub ust. 2 Umowy Kupującemu przysługuje kara umowna w wysokości 2 000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia.
2. Jeśli opóźnienie, o którym mowa w ust. 1 trwało będzie dłużej niż 14 dni, Kupujący może, bez wyznaczenia dodatkowego terminu, odstąpić od Umowy (w terminie 14 dni od wystąpienia przesłanki uprawniającej do odstąpienia) oraz zażądać kary umownej w wysokości 20% kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy.
3. W przypadku opóźnienia Sprzedawcy w wymianie Sprzętu IT na fabrycznie nowy, wolny od wad w okresie Serwisu gwarancyjnego (gwarancji) lub rękojmi, w stosunku do terminów, o którym mowa w § 6 ust. 4 lub 5 Umowy, Kupującemu przysługuje kara umowna w wysokości 0,1% kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy za każdy rozpoczęty dzień kalendarzowy, jeżeli termin liczony jest w dniach lub odpowiednio kara umowna w wysokości 0,02% kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy, za każdą rozpoczętą godzinę opóźnienia, jeżeli termin liczony jest w godzinach.
4. Jeżeli opóźnienie, o którym mowa w ust. 3 trwało będzie dłużej niż 24 godziny (dla terminów liczonych w godzinach) lub odpowiednio 3 dni (dla terminów liczonych w dniach), Kupujący, w terminie 14 dni od upływu terminu powyższego opóźnienia, ma prawo, według własnego wyboru:
   1) odstąpić od Umowy bez konieczności wyznaczania dodatkowego terminu na usunięcie wad oraz żądać kary umownej w wysokości 20% kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy,
   2) dokonać zastępczej wymiany Sprzętu IT na koszt Sprzedawcy,
   3) naliczyć 2-krotność kary umownej określonej w ust. 3, począwszy odpowiednio od 25 godziny opóźnienia lub od 4 dnia opóźnienia, do terminu, w którym zostanie wymieniony Sprzęt IT.
5. W przypadku opóźnienia Sprzedawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia, w stosunku do terminu, o którym mowa w § 4 ust. 8, Sprzedawca zapłaci karę umowną w wysokości 2 000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień opóźnienia.
6. W przypadku opóźnienia Sprzedawcy w odbiorze Sprzętu IT wraz z Oprogramowaniem i Dokumentów z miejsca dostarczenia, w stosunku do terminu, o którym mowa w § 4 ust. 9, Sprzedawca zapłaci karę umowną w wysokości 2 000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia. W przypadku ponownej odmowy odbioru Sprzętu IT, o której mowa w § 4 ust. 9 Umowy, Kupujący ma prawo odstąpić od Umowy w terminie 30 dni od daty przekazania Sprzedawcy protokołu odmowy odbioru Sprzętu IT i żądać kary umownej w wysokości 20 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy, z zachowaniem prawa do kary umownej określonej w zdaniu poprzednim, naliczonej do dnia odstąpienia.
7. W przypadku opóźnienia Sprzedawcy w dostarczeniu Kupującemu Dokumentacji powykonawczej w stosunku do terminu o którym mowa w § 4 ust. 10 Sprzedawca zapłaci karę umowną w wysokości 2 000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia.
8. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną, bądź szkoda powstanie z innych przyczyn niż te, dla których zastrzeżono karę, Kupującemu przysługuje prawo do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
9. Kary umowne płatne są w terminie 14 dni od daty otrzymania wezwania. Niezależnie od powyższego kary umowne mogą być potrącane z wynagrodzenia należnego Sprzedawcy lub z zabezpieczenia należytego wykonania Umowy.

§ 9. Prawa autorskie

1. Sprzedawca zapewnia, że korzystanie przez Kupującego z Dokumentacji powykonawczej nie będzie naruszało praw osób trzecich. Na podstawie Umowy Sprzedawca przeniesie na Kupującego autorskie prawa majątkowe w zakresie i w sposób opisany poniżej.
2. Z dniem podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy, Sprzedawca przenosi na Kupującego autorskie prawa majątkowe do Dokumentacji powykonawczej, na polach eksploatacji wskazanych w ust. 3, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy.
3. Przeniesienie autorskich praw majątkowych do utworów, o których mowa w niniejszym paragrafie, obejmuje następujące pola eksploatacji:
   1) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie każdą techniką egzemplarzy utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
   2) w zakresie obrotu oryginałem oraz egzemplarzami, na których utwory utrwalono – wprowadzanie do obrotu, użyczanie oraz najem oryginału oraz egzemplarzy;
   3) w zakresie rozpowszechniania utworów w sposób inny niż określony w pkt. 2 – publiczne wykonanie, wystawienie, wyświetlanie, odtwarzanie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
   4) dowolne przetwarzanie utworów, w tym łączenie z innymi utworami;

5) zezwalanie na wykonywanie zależnych praw autorskich poprzez rozporządzanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt. 1-4.

4. Z dniem dokonania przez Kupującego odbioru Dokumentacji powykonawczej, Kupujący nabywa własność nośników, na których utwory te utrwalono, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy.

§ 10. Wady prawne

1. Sprzedawca gwarantuje, że Sprzęt IT, Oprogramowanie, Dokumenty oraz Dokumentacja powykonawcza nie naruszają praw własności intelektualnej ani innych praw osób trzecich.
2. W przypadku wystąpienia osób trzecich wobec Kupującego z roszczeniami opartymi na twierdzeniu, iż używany przez Kupującego Sprzęt IT, Oprogramowanie, Dokumenty lub Dokumentacja powykonawcza naruszają jakiekolwiek prawa, o których mowa w ust. 1, Kupującemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub osobno):
   1) prawo odstąpienia od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach z wyłączeniem zapłaty na rzecz Sprzedawcy jakichkolwiek kosztów, odszkodowań itp.,
   2) prawo żądania zapłaty przez Sprzedawcę kary umownej w wysokości 20% łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy oraz prawo żądania odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.
3. W przypadku wytoczenia przeciwko Kupującemu powództwa opartego na twierdzeniu opisanym w ust. 2, Sprzedawca zobowiązuje się zapewnić Kupującemu na swój koszt ochronę sądową oraz ponieść konsekwencje zapadłego wyroku sądowego.

§ 11. Zabezpieczenie należytego wykonania Umowy (dalej: „**ZNWU**")

1. Sprzedawca złożył u Kupującego ZNWU w jednej z form, o których mowa w art. 148 ust. 1 ustawy Prawo zamówień publicznych w wysokości ..... zł (słownie złotych: ..... XX/100).
2. ZNWU dotyczy pokrycia ewentualnych roszczeń wynikających z niewykonania lub nienależytego wykonania Umowy.
3. ZNWU zostanie zwolnione (zwrócone):
   1) w wysokości 70% zabezpieczenia w terminie 30 dni od dnia podpisania bez zastrzeżeń Protokołu odbioru, o którym mowa w § 4 ust. 7 Umowy,
   2) w wysokości 30 % zabezpieczenia w terminie 15 dni po upływie okresu Serwisu gwarancyjnego i rękojmi.
4. W przypadku zmiany formy ZNWU w trakcie trwania Umowy obowiązywać będą poniższe zasady.
5. ZNWU w formie pieniężnej Sprzedawca wpłaca przelewem na rachunek bankowy wskazany przez Kupującego.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz Kupującego w terminie 30 dni od pisemnego żądania kwotę ..... zł (słownie złotych: ..... XX/100), na pierwsze wezwanie Kupującego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Sprzedawcy i bez dochodzenia czy wezwanie Kupującego jest uzasadnione czy nie.
7. ZNWU wnoszone w formie poręczenia ma być wystawione przez bank, spółdzielczą kasę oszczędnościowo-kredytową lub podmiot, o którym mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, który poręczy należyte wykonanie Umowy do wysokości ..... zł (słownie złotych: ..... XX/100).
8. W przypadku, gdy ZNWU, o którym mowa w ust.1 będzie wnoszone w formie: poręczenia, bankowej lub ubezpieczeniowej gwarancji, Kupujący zastrzega sobie prawo do akceptacji projektu tych dokumentów.
9. ZNWU wniesione w formie pieniężnej podlega zwrotowi wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek Sprzedawcy.
10. ZNWU w formie innej niż pieniężna Sprzedawca złoży u Kupującego w Kancelarii Głównej, Warszawa ul. Poleczki 33, z dopiskiem „*Dla Departamentu Informatyki*".

§ 12. Odstąpienie od Umowy

1. Strony mogą odstąpić od Umowy w przypadkach przewidzianych obowiązującymi przepisami, a także w przypadku zaistnienia okoliczności, o których mowa w Umowie.
2. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Kupujący może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Sprzedawca może żądać jedynie wynagrodzenia należnego z tytułu wykonania części Umowy.
3. Przy wykonaniu Umowy Sprzedawca bez zgody Kupującego nie ma prawa do korzystania w jakimkolwiek charakterze z osób zatrudnionych u Kupującego, pod rygorem odstąpienia od Umowy przez Kupującego z winy Sprzedawcy w terminie 30 dni od powzięcia wiadomości o zaistnieniu takiego faktu oraz żądania zapłaty kary umownej, o której mowa w ust. 4.
4. W wyniku wystąpienia okoliczności, o której mowa w ust. 3 Sprzedawca jest zobowiązany do zapłaty w terminie 14 dni od wezwania przez Kupującego kary umownej w wysokości 20 000,00 zł (słownie złotych: dwadzieścia tysięcy 00/100). Jeżeli szkoda poniesiona przez Kupującego jest wyższa od zastrzeżonej wyżej kary umownej, Kupujący może dochodzić odszkodowania uzupełniającego od Sprzedawcy na zasadach ogólnych Kodeksu cywilnego.
5. Wszelkie zmiany treści Umowy wymagają formy pisemnej pod rygorem nieważności, za wyjątkiem tych, dla których w Umowie zastrzeżono inną formę.

§ 13. Zawiadomienia

1. Wszelkie zawiadomienia wymienione w Umowie, niezależnie od nazwy, pod którą występują, dla swojej skuteczności Strony muszą przekazać osobiście za potwierdzeniem odbioru lub pocztą poleconą za zwrotnym poświadczeniem ich odbioru i będą uważane za skutecznie doręczone w dniu ich odbioru, z zastrzeżeniem § 6 ust. 6 Umowy.
2. Zawiadomienia, zapytania, informacje nie wymienione w postanowieniach Umowy mogą być przesyłane telefaksem, doręczane osobiście, przesyłane kurierem lub listem, pod warunkiem ich potwierdzenia przez drugą Stronę.
3. Zawiadomienia będą wysyłane na adresy Stron wskazane w komparycji Umowy. Każda ze Stron zobowiązana jest do informowania drugiej Strony o każdej zmianie adresu. Jeżeli Strona nie powiadomiła o zmianie adresu, zawiadomienia wysłane na ostatni znany adres Strony uznają za doręczone. Powiadomienie o powyższych zmianach nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.

§ 14. Poufność, bezpieczeństwo informacji i zasady przetwarzania danych osobowych

1. Wszelkie wiadomości dotyczące Stron Umowy oraz warunków Umowy, w których posiadanie weszła druga Strona przy zawieraniu i wykonywaniu Umowy mają charakter poufny. Każda ze Stron zobowiązuje się nie ujawniać ich osobom trzecim, także po zakończeniu Umowy, wyjąwszy przypadki przewidziane prawem.
2. Sprzedawca zobowiązuje się do zapoznania się i przestrzegania przyjętych u Kupującego zasad bezpieczeństwa informacji, których treść została określona w Załączniku nr 6 (Regulamin bezpieczeństwa fizycznego i środowiskowego) i nr 12 (Regulamin eksploatacji systemów teleinformatycznych) do Zarządzenia nr 78/2019 w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR, które stanowią Załącznik nr 5a do Umowy.
3. Sprzedawca potwierdza fakt zapoznania się, w zakresie dotyczącym Umowy, z Załącznikami nr 6 i nr 12 do Zarządzenia, o którym mowa w ust. 2 podpisując oświadczenie. Wzór oświadczenia stanowi Załącznik nr 5b do Umowy.
4. Sprzedawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) oraz przepisów krajowych wydanych w związku z ogólnym rozporządzeniem o ochronie danych, zwanym dalej: „RODO".
5. Sprzedawca pisemnie zobowiąże pracowników i osoby trzecie realizujące zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 2 i 4.
6. Sprzedawca oświadcza, że zapoznał się z klauzulą informacyjną w zakresie przetwarzania danych osobowych, stanowiącą Załącznik nr 6a do Umowy.
7. Sprzedawca zobowiązuje się do złożenia oświadczenia o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane bezpośrednio lub pośrednio pozyskał w celu zawarcia oraz wykonania Umowy zgodnie z wzorem oświadczenia stanowiącym Załącznik nr 6b do Umowy.

§ 15. Postanowienia końcowe

1. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu cywilnego, ustawy Prawo zamówień publicznych oraz ustawy o prawie autorskim i prawach pokrewnych.
2. Ewentualne spory mogące wyniknąć na tle wykonania Umowy rozstrzygać będzie sąd powszechny właściwy dla siedziby Kupującego.
3. Sprzedawca nie może bez zgody Kupującego przenieść praw wynikających z Umowy na osoby trzecie.
4. Załączniki wymienione w Umowie stanowią jej integralną część.
   Poniżej przedstawiono spis załączników:
   1) Załącznik nr 1 – Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia;
   2) Załącznik nr 2 – Protokół odbioru (wzór);
   3) Załącznik nr 3 – Protokół odbioru Dokumentacji powykonawczej (wzór);
   4) Załącznik nr 4a – Protokół usunięcia wady (wzór);
   5) Załącznik nr 4b – Protokół odbioru konsultacji (wzór);
   6) Załącznik nr 5a – Treść Załączników nr 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR;
   7) Załącznik nr 5b – Oświadczenie o zapoznaniu się z treścią Załączników nr 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR;
   8) Załącznik nr 6a – Klauzula informacyjna dotycząca przetwarzania danych osobowych;
   9) Załącznik nr 6b – Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO (wzór);
   10) Załącznik nr 7 – Formularz ofertowy;
   11) Załącznik nr 8 – Wykaz osób.
5. Umowę sporządzono w 4 jednobrzmiących egzemplarzach, w tym jeden dla Sprzedawcy i trzy dla Kupującego.

Sprzedawca **Kupujący**

....

....

Załącznik nr 1 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia

1. Firewall'e – 2 szt., każde spełniające następujące wymagania minimalne

Lp.	Wymagania minimalne
1	1. Firewall musi być dostarczony jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". 2. Całość Sprzętu IT musi być zarządzana przez jednego producenta
2	Firewall musi być wyposażony w: 1. 4 interfejsy 100/1000/10GE Ethernet (RJ45) 2. 16 interfejsów 1/10GE SFP+ (z czego 12 interfejsów obsadzonych modułami 10GE SFP+ SR) 3. 4 interfejsy 40GE/100GE QSFP+ lub alternatywnie 4 interfejsy 40GE QSFP+ i 4 interfejsy 100GE QSFP+
3	Firewall musi być wyposażony w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1).
4	Firewall musi być wyposażony w dedykowany port konsoli/zarządzania. Port ten musi być wydzielony logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji.
5	Firewall musi spełniać następujące parametry wydajnościowe, jeżeli Firewall może pracować w różnych trybach to jego wydajność musi być mierzona w trybie pracy, który pozwala na uruchomienie wszystkich wymaganych funkcji Sprzętu IT: 1. minimum 40 Gbps dla Firewall/kontroli aplikacji; 2. minimum 20 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji; 3. minimum 280 tys. nowych połączeń na sekundę; 4. minimum 8 000 000 równoległych sesji.
6	Firewall musi umożliwiać działanie w trzech trybach pracy: 1. rutera (tzn. w warstwie 3 modelu OSI); 2. przełącznika (tzn. w warstwie 2 modelu OSI); 3. w trybie pasywnego nasłuchu (sniffer).
7	Tryb pracy Firewall-a musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).
8	1. Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN. 2. Firewall musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. 3. Firewall musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
9	1. Firewall musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. 2. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
10	1. Firewall musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. 2. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). 3. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN
11	1. Firewall musi spełniać następujące parametry wydajnościowe: a) minimum 15Gbps b) minimum 10 000 tuneli IPSEC VPN (site-to-site) c) minimum 15 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. 2. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji lub jeżeli dedykowany klient VPN (dla systemów: Windows, Linux, Android, MacOS) oferowany przez producenta Sprzętu IT wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 15 000 jednoczesnych użytkowników..
12	Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach: 1. Polityki definiujące powinny umożliwiać wykorzystanie: a) adresów źródłowych b) adresów docelowych c) użytkowników d) numerów portów usług e) kategorie URL 2. System musi obsługiwać następujące mechanizmy uwierzytelnienia a) RADIUS lub TACACS+ b) LDAP c) Kerberos lub SAML 2.0
13	Firewall musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie: 1. oznaczania pakietów znacznikami DiffServ; 2. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego; 3. utworzenia 8 klas ruchu sieciowego; 4. kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników; 5. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP; 6. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego..
14	Firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP
15	Firewall musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.

16	1. Firewall musi obsługiwać nie mniej niż 50 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. 2. Kupujący dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych).
17	Firewall musi obsługiwać nie mniej niż 25 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 75 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: 1. tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych); 2. Polityk bezpieczeństwa obejmujących: d) System IPS; e) System ochrony antymalware/antyspyware; f) System ochrony antywirus; 1. Koncentratorów VPN dla zdalnego dostępu.
18	Firewall musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu
19	1. Firewall musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie firewall-i. 2. Firewall-e w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
20	1. Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. 2. Firewall musi umożliwiać zdefiniowanie nie mniej niż 50 000 reguł polityki bezpieczeństwa.
21	1. Identyfikacja aplikacji musi odbywać się poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji Sprzętu IT numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. 2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych. 3. Firewall musi wykrywać 2500 predefiniowanych aplikacji wspieranych przez producenta (w szczególności: Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na Sprzęcie IT bez użycia zewnętrznych narzędzi
22	1. Firewall musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. 2. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
23	1. Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. 2. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
24	1. Firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. 2. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia..
25	1. Firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. 2. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
26	Firewall musi zapewniać ochronę przed atakami typu „Drive-by-download".
27	1. Firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. 2. Wymagana jest obsługa deszyfracji i inspekcji protokołu HTTP/2 zarówno dla ruchu inbound jak i outbound.
28	Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH
29	Firewall musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: 1. Microsoft Active Directory; 2. usługi katalogowe LDAP; 3. serwery Terminal Services.
30	Polityka kontroli dostępu Firewall-a musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
31	1. Firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. 2. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. 3. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w Firewall który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.
32	1. Firewall musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. 2. System IPS musi działać w warstwie 7 modelu OSI. 3. Baza sygnatur IPS/IDS musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent Sprzętu IT. 4. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby

	funkcja IPS/IDS uruchamiana była per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi.
33	1. Firewall musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. 2. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder, w szczególności: http, smtp, imap, pop3, ftp, smb. 3. Baza sygnatur AV musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń 4. Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. 5. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
34	1. Firewall musi zapewniać ochronę przed atakami typu Spyware – dopuszcza się by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. 2. Baza sygnatur anty-spyware musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. 3. Reguły/silnik anty-spyware musi być uruchamiany per reguła polityki bezpieczeństwa firewall. 4. Nie jest dopuszczalne, aby funkcja ta była uruchamiana per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi i wsparcia producenta. 6. Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania
35	1. Firewall musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). 2. Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
36	Firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
37	1. Firewall musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. 2. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. 3. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. 4. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 6. Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania
38	1. Firewall musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem. 2. Firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. 3. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to nie wymagane jest jej dostarczenie w chwili zakupu Firewalla/i.
39	1. Zarządzanie Firewall-em musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę www. 2. Dostęp do Firewall-a i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
40	1. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. 2. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą: d) bazy lokalnej; e) serwera LDAP; f) RADIUS lub TACACS+. 3. Firewall musi zapewniać tworzenie sekwencji uwierzytelniającej posiadającej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
41	Firewall musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu Firewall-a bez użycia systemu zarządzania lub linii poleceń (CLI).
42	Firewall musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym Firewall-a
43	Firewall musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
44	Firewall musi umożliwiać bieżące wysyłanie logów do zewnętrznych serwerów SYSLOG oraz posiadać możliwość wysyłania logów z wykorzystaniem protokołu TCP i zdefiniowana portu docelowego.
45	Firewall musi być wyposażony w zasilacze typu AC pracujące redundantnie

System zarządzania:

Lp.	Wymagania minimalne
1	1. Wraz urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania. 2. Dopuszcza się budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta Firewall-i i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. 3. System zarządzania musi pracować w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów.
2	System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMWare.
3	System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne: 1. obsługa nie mniej niż 10 firewalli fizycznych 2. obsługa nie mniej niż 10 firewalli wirtualnych 3. zapewnienie obsługi przestrzeni dyskowej o pojemności nie mniejszej niż 10 TB. 4. Możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczonej na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji)
4	1. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach www. 2. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli
5	System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym: 1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 2. tworzenie statycznych raportów dopasowanych do wymagań Kupującego. 3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 4. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Kupującego z funkcjonalnością „drill-down".
6	System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym: 1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. a) lokalnych (dla wybranych firewalli lub logicznych systemów firewalla). b) globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). 2. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów) 3. pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń. 4. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. 5. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 6. umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
7	System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym musi: 1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu; 2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli; 3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur; 4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem; 5. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów; 6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone; 7. informować o zmianach konfiguracji systemu.
8	System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.

2. W ramach Wdrożenia Sprzedawca wykona następujące czynności:

1) zainstaluje Sprzęt IT i Oprogramowanie w COPD, w wskazanym przez Kupującego miejscu, przy czym instalacja obejmuje dostawę i montaż kabli logicznych i zasilających;
2) podłączy Sprzęt IT do sieci zasilającej i sieci logicznej, zainstaluje Oprogramowanie oraz skonfiguruje w sposób umożliwiający uzyskanie przez Kupującego dostępu do kompletnie skonfigurowanych oraz widocznych dla administratora zasobów Sprzętu IT z poziomu GUI;
3) uruchomi Sprzęt IT oraz przedstawi, na życzenie Kupującego, poszczególne lub wszystkie funkcjonalności Sprzętu IT i Oprogramowanie, o których mowa w niniejszym Załączniku oraz w Załączniku nr 7 do Umowy.
4) przygotuje konfigurację Sprzętu IT (konfiguracja klastra rozciągniętego na dwie lokalizacje);
5) dokona migracji z urządzeń PA5060 dotychczas użytkowanych 2 szt. appliance wraz z przeniesieniem wszystkich funkcji zaimplementowanych na ww. urządzeniach;
6) uruchomi i zaprezentuje w celach testowych wybrane przez Kupującego funkcjonalności;
7) zainstaluje Sprzęt IT i skonfiguruje Oprogramowanie w COPD;
8) uruchomi Sprzęt IT produkcyjnie z funkcjonalnościami wskazanymi przez Kupującego;
9) dokona instruktażu obsługi wdrożonych Sprzętu IT dla 10 pracowników Kupującego, czas trwania instruktażu wyniesie do 5 Dni Roboczych.

Załącznik nr 2 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Protokół odbioru
(wzór)

Zgodnie z Umową nr ...../DI/2019/2610 zawartą w dniu ..... 2019 r. pomiędzy Agencją Restrukturyzacji i Modernizacji Rolnictwa (Kupujący) a ....., Kupujący potwierdza, że Sprzedawca dostarczył Sprzęt IT/Oprogramowanie i wykonał Wdrożenie zgodnie z Umową:

Lp.	*Nazwa Sprzętu IT/Oprogramowania*	**Ilość**	*Numer seryjny/wersja**

Upoważnieni przedstawiciele Kupującego i Sprzedawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że:

1. Dostarczony Sprzęt IT wraz z Oprogramowaniem jest fabrycznie nowy i nie nosi śladów uszkodzeń zewnętrznych oraz uprzedniego używania. Ilość oraz rodzaj dostarczonego Sprzętu IT wraz z Oprogramowaniem jest zgodny z Umową.
2. Dostarczony Sprzęt IT oraz Oprogramowanie są wolne od oprogramowania szkodliwego i szpiegującego, a także są zabezpieczone przed nieautoryzowanym dostępem.
3. Wraz ze Sprzętem IT dostarczono wszystkie wymagane Dokumenty (instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania).
4. Dokonano usunięcia i utylizacji wszelkich opakowań pozostałych po rozpakowaniu Sprzętu IT.
5. Wykonano Wdrożenie prawidłowo, zgodnie z Umową.

Uwagi i zastrzeżenia:

Kupujący (upoważniony przedstawiciel)			**Sprzedawca** (upoważniony przedstawiciel)
.....			.....
.....			.....

....., dnia ..... 2019 roku

* - niepotrzebne skreślić

Załącznik nr 3 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Protokół odbioru Dokumentacji powykonawczej
(wzór)

Dane dokumentu

Nazwa projektu + **Lokalizacja** **Kierownik Sprzedawcy:**	**Numer wersji dokumentu:** **Data wersji dokumentu:**

UWAGI:

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

Kupujący odbiera / nie odbiera*
Dokumentację *

Kupujący (upoważniony przedstawiciel)		**Sprzedawca** (upoważniony przedstawiciel)	
Imię i nazwisko:		**Imię i nazwisko:**	
Stanowisko:		**Stanowisko:**	
Data:		**Data:**	
Podpis:		**Podpis:**	

* - niewłaściwe skreślić.

Załącznik nr 4a do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Protokół odbioru usunięcia wady
(wzór)

1. Imiona i nazwiska osób dokonujących czynności odbioru:

2. Wyszczególnienie odbieranych czynności w ramach usuniętych wad:

3. Data podpisania protokołu: ..... r.

4. Podpisy

.....	.....
Kupujący	Sprzedawca
(upoważniony przedstawiciel)	(upoważniony przedstawiciel)

Załącznik nr 4b do umowy nr _____/DI/2019/2610 z dnia _____.2019 r.

Protokół odbioru konsultacji
(wzór)

1. Opis konsultacji w kwartale _____

   _____
   _____
   _____

2. Ilość wykorzystanych godzin _____

3. Uwagi/zastrzeżenia

   _____
   _____

4. Podpisy

Sprzedawca	**Kupujący**
(upoważniony przedstawiciel)	*(upoważniony przedstawiciel)*
.....	.....
.....	.....

Warszawa, dnia _____ r.

Załącznik nr 5a do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Oświadczenie
o zapoznaniu się z treścią Zarządzenia Prezesa ARiMR
nr 78/2019 w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR

Sprzedawca oświadcza, że zapoznał się z treścią Załączników nr 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019 z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR i zobowiązuje się do przestrzegania ich postanowień podczas realizacji Umowy.

. . . . . .
(podpis i pieczęć osoby (osób) upoważnionej
do reprezentowania Sprzedawcy)

Warszawa., dn. . . . . .2019 r.

Załącznik nr 5b do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Treść Załączników nr 6 i 12 do Zarządzenia Prezesa ARiMR nr 78/2019
z dnia 3 czerwca 2019 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji w ARiMR

Załącznik nr 6a do umowy nr _____/DI/2019/2610 z dnia _____.2019 r.

Klauzula informacyjna dotycząca przetwarzania danych osobowych

W związku z treścią z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) („Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), dalej: „RODO" Kupujący informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator danych) pozyskanych w związku z zawarciem Umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II, 00-175 Warszawa. Z Administratorem danych można kontaktować się poprzez e-mail: info@arimr.gov.pl lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
2. Administrator danych wyznaczył inspektora ochrony danych, z którym można kontaktować się w sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, poprzez adres e-mail: iod@arimr.gov.pl lub pisemnie na adres korespondencyjny Administratora danych, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora danych przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu zawarcia oraz wykonania Umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
   1) organy kontrolne,
   2) osoby lub podmioty, którym Administrator danych udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 poz. 1330 z późn. zm.),
   3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
   4) podmioty przetwarzające dane osobowe w imieniu Administratora danych na mocy zawartych innych umów, m. in. dostawcy IT.
5. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania Umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych będzie niezbędne do dochodzenia roszczeń lub do obrony przed takimi roszczeniami przez Administratora danych. Ponadto, okres przechowywania danych może zostać przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych oraz prawo do przenoszenia Pani/Pana danych osobowych.
7. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Panią/Pana danych osobowych jest konieczne w celu określonym w pkt 3 powyżej, dla zawarcia i wykonania Umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa, a konsekwencją niepodania Pani/Pana danych osobowych będzie brak możliwości zawarcia Umowy.

Załącznik nr 6b do umowy nr _____/DI/2019/2610 z dnia _____.2019 r.

Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO
(wzór)

..... z siedzibą w i adresem ul. ....., zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonym przez Sąd Rejonowy ....., Wydział .....Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS ....., o numerze Regon ....., zarejestrowanym podatnikiem podatku od towarów i usług NIP ....., kapitał zakładowy ..... zł, którą reprezentuje:

1. .....,
2. .....,

zwana „Sprzedawcą"

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu zawarcia oraz wykonania Umowy[2].

(podpisy)

1. .....,
2. .....,

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2).
[2] W przypadku, gdy Sprzedawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Sprzedawca nie składa.

Załącznik nr 7 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Formularz ofertowy

Załącznik nr 8 do Umowy nr _____/DI/2019/2610 z dnia _____ 2019 r.

Wykaz osób
(zgodny ze złożonym w postępowaniu)

Doświadczenie osób wyznaczonych do realizacji zamówienia, o których mowa w § 3 ust. 5 Umowy:

1. osoba z co najmniej 12 miesięcznym doświadczeniem przy realizacji zamówień na dostawy urządzeń typu Firewall (urządzenia pełniące funkcje zapory ogniowej), wraz z wdrożeniem, posiadająca certyfikat Cisco Certified Internetwork Expert (CCIE) Security lub równoważny.

Załącznik nr 7 do SIWZ

Plik, w formacie xml, wygenerowany z narzędzia ESPD

Plik, w formacie xml, wygenerowany z narzędzia ESPD („ESPD") znajduje się w odrębnym pliku o nazwie „Załącznik nr 7 do SIWZ ESPD". Plik należy pobrać i zapisać na dysk komputera oraz wypełnić przy pomocy narzędzia udostępnionego przez Urząd Zamówień Publicznych pod adresem https://espd.uzp.gov.pl .

Po uruchomieniu wyżej wymienionej strony internetowej, należy wybrać „pl Polski", a potem zaznaczyć „Jestem wykonawcą". Następnie należy zaimportować „ESPD" wczytując plik będący Załącznikiem nr 7 do SIWZ. Po sporządzeniu JEDZ należy go podpisać przez osobę lub osoby uprawnione.

Aktualne na dzień składania ofert oświadczenie w formie jednolitego europejskiego dokumentu zamówienia należy złożyć w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, za pomoca środka komunikacji elektronicznej tj. Platformę Zakupową.

Szczegółowy zakres wymagań określony został w Rozdziale IV.2 SIWZ.