



# Specyfikacja Warunków Zamówienia

*w postępowaniu o udzielenie zamówienia publicznego  
o wartości równej lub przekraczającej progi unijne  
prowadzonym w trybie przetargu nieograniczonego*

**na:**

**„Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami”**

**numer referencyjny sprawy: DPiZP.2610.10.2021**

wszczętym na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.)

<b>Informacje dotyczące prowadzonego postępowania o udzielenie zamówienia publicznego</b> .....	<b>3</b>
A. Dane Zamawiającego .....	3
B. Pozostałe informacje dotyczące prowadzonego postępowania .....	3
<b>Rozdział I. Przedmiot zamówienia</b> .....	<b>5</b>
I.1. Opis przedmiotu zamówienia.....	5
I.2. Opis części zamówienia .....	12
I.3. Powierzenie Podwykonawcy wykonania części zamówienia.....	12
I.4. Pozostałe istotne elementy związane z przedmiotem zamówienia.....	12
<b>Rozdział II. Termin wykonania zamówienia</b> .....	<b>12</b>
<b>Rozdział III. Podstawy wykluczenia oraz warunki udziału w postępowaniu, jednolity europejski dokument zamówienia</b> .....	<b>12</b>
III.1. Podstawy wykluczenia.....	13
III.2. Warunki udziału w postępowaniu.....	14
<b>Rozdział IV. Zawartość ofert, wykaz podmiotowych środków dowodowych</b> .....	<b>15</b>
IV.1. Zawartość ofert .....	15
IV.2 Oświadczenie w formie Jednolitego Europejskiego Dokumentu Zamówienia .....	16
IV.3. Wykaz podmiotowych środków dowodowych .....	16
IV.4. Podmiotowe środki dowodowe składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej .....	17
IV.5. Zasady i warunki korzystania przez Wykonawcę ze zdolności lub sytuacji innych podmiotów .....	17
IV.6. Klauzule informacyjne w zakresie danych osobowych.....	18
<b>Rozdział V. Informacje o sposobie porozumiewania się zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do komunikowania się z Wykonawcami</b> .....	<b>18</b>
<b>Rozdział VI. Wymagania dotyczące wadium</b> .....	<b>19</b>
<b>Rozdział VII. Termin związania ofertą</b> .....	<b>19</b>
<b>Rozdział VIII Opis sposobu przygotowywania ofert</b> .....	<b>19</b>
VIII.1. Przygotowanie ofert.....	19
VIII.2. Forma dokumentów składanych w postępowaniu .....	20
<b>Rozdział IX. Sposób oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty</b> .....	<b>21</b>
IX.1. Sposób oraz termin składania ofert i otwarcia ofert .....	21
IX.2. Warunki zmiany i wycofania złożonej oferty.....	21
<b>Rozdział X. Opis sposobu obliczenia ceny</b> .....	<b>21</b>
<b>Rozdział XI. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert</b> .....	<b>22</b>
<b>Rozdział XII. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego</b> .....	<b>22</b>
<b>Rozdział XIII. Wymagania dotyczące zabezpieczenia należytego wykonania umowy</b> .....	<b>23</b>
<b>Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego</b> .....	<b>24</b>
<b>Rozdział XV. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia publicznego</b> .....	<b>24</b>
<b>Załączniki do SWZ:</b> .....	<b>25</b>
<i>Załącznik nr 1 -1A do SWZ – wzór Formularza Ofertowego</i> .....	26
<i>Załącznik nr 2 do SWZ – wzór Oświadczenia o braku podstaw wykluczenia</i> .....	30
<i>Załącznik nr 3 do SWZ – wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej</i> .....	35
<i>Załącznik nr 4 do SWZ – wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia</i> .....	36
<i>Załącznik nr 5 do SWZ – wzór Oświadczenia – Wykaz usług</i> .....	37
<i>Załącznik nr 6 do SWZ – projektowane postanowienia umowy</i> .....	40
<i>Załącznik nr 7 do SWZ – plik, w formacie XML, wygenerowany z narzędzia ESPD</i> .....	73

## Informacje dotyczące prowadzonego postępowania o udzielenie zamówienia publicznego

### A. Dane Zamawiającego

#### 1. Zamawiającym jest:

Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie (adres: Al. Jana Pawła II 70, 00-175 Warszawa); adres do korespondencji: ul. Poleczki 33, 02-822 Warszawa, tel. 22 595 06 11, adres e-mail: [zamowieniapubliczne@arimr.gov.pl](mailto:zamowieniapubliczne@arimr.gov.pl);

REGON: 010613083;

NIP: 526-19-33-940.

#### 2. Adres strony internetowej prowadzonego postępowania o udzielenie zamówienia publicznego (dalej: „postępowanie”): <https://platformazakupowa.pl/pn/arimr>.

#### 3. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 z późn. zm.; dalej: „ustawa”).

### B. Pozostałe informacje dotyczące prowadzonego postępowania

#### 1. Zmiany i wyjaśnienia treści Specyfikacji Warunków Zamówienia (dalej: „SWZ”) oraz inne dokumenty zamówienia bezpośrednio związane z niniejszym postępowaniem będą zamieszczane na stronie internetowej pod adresem <https://platformazakupowa.pl/pn/arimr> gdzie należy wybrać zakładkę „postępowania”, a następnie przejść na formularz niniejszego postępowania.

#### 2. Postępowanie 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”).

#### 3. Poniżej Zamawiający przedstawia wymagania techniczno-organizacyjne związane z udziałem Wykonawców w postępowaniu:

3.1. Złożenie oferty możliwe jest przez Wykonawców, którzy posiadają konto na Platformie Zakupowej oraz przez Wykonawców nieposiadających konta na Platformie Zakupowej. W celu założenia konta na Platformie Zakupowej należy wybrać zakładkę „Zaloguj się” w kolejnym kroku należy wybrać „Założ 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 i nr telefonu.

3.2. Złożenie oferty oraz oświadczenia, o którym mowa w art. 125 ustawy, składanych w trakcie toczącego się postępowania wymaga od Wykonawcy posiadania kwalifikowanego podpisu elektronicznego.

3.3. 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.

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

#### 4. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (t.j. Dz. U. z 2020 r. poz. 2452; dalej: „Rozporządzenie w sprawie środków komunikacji”), udostępni informacje na temat specyfikacji połączenia, formatu przesyłanych danych oraz szyfrowania i oznaczania czasu przekazania i odbioru danych umożliwiających pracę na Platformie Zakupowej, tj.:

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

4.2. 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,

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

4.4. włączona obsługa JavaScript,

4.5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików PDF.

4.6. Platforma Zakupowa działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,

#### 5. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia w sprawie środków komunikacji, określa dopuszczalne formaty przesyłanych danych, tj. plików o wielkości do 150 MB. Zalecany format: PDF.

#### 6. Zamawiający, zgodnie z § 11 ust. 2 Rozporządzenia w sprawie środków komunikacji, określa informacje na temat szyfrowania oraz czasu przekazania i odbioru danych, tj.:

6.1. Szyfrowanie na Platformie Zakupowej ([platformazakupowa.pl](https://platformazakupowa.pl)) odbywa się za pomocą protokołu TLS 1.3.

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

6.3. Oznaczenie czasu przekazania i odbioru danych przez Platformę Zakupową 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 określa dopuszczalny format kwalifikowanego podpisu elektronicznego w przypadku:

- 7.1. dokumentów sporządzonych w formacie PDF zaleca się podpisanie dokumentu podpisem w formacie PAdES;
- 7.2. dokumentów sporządzonych w formacie innym niż PDF zaleca się podpisanie dokumentu podpisem w formacie XAdES.
8. Wykonawca przystępując do niniejszego postępowania 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 SWZ, 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 8:00 do 17:00 w dni robocze od poniedziałku do piątku pod numerem telefonu 22 101 02 02 lub e-mai: [cwk@platformazakupowa.pl](mailto:cwk@platformazakupowa.pl).

## Rozdział I. Przedmiot zamówienia

### I.1. Opis przedmiotu zamówienia

1. Kod Wspólnego Słownika Zamówień (CPV).
  - 1.1. Główny kod: 51610000-1 [Usługi instalowania urządzeń komputerowych i przetwarzania informacji];
  - 1.2. Dodatkowy kod: 48732000-8 [Pakiety oprogramowania do zabezpieczania danych];  
32420000-3 [Urządzenia sieciowe];  
72220000-3 [Usługi doradcze w zakresie systemów i doradztwo techniczne].
2. Przedmiotem zamówienia jest zakup wraz z dostawą i wdrożeniem 2 sztuk fabrycznie nowych, takich samych, nienoszących śladów poprzedniego użytkowania urządzeń informatycznych pełniących funkcje zapory rdzenia o parametrach i funkcjonalnościach określonych w specyfikacji technicznej wskazanej poniżej w pkt 2.1. oraz stanowiącej Załącznik nr 1 do projektowanych postanowień umowy (dalej: ppu) wraz z załącznikami stanowiącej Załącznik nr 7 do Specyfikacji Warunków Zamówienia (dalej: SWZ).
  - 2.1. Zamawiający posiada w swojej infrastrukturze skonfigurowane zapory sieciowe Palo Alto PA-5250 oraz system zarządzania Panorama w związku z tym wymaga dostarczenia 2 sztuk urządzeń Palo Alto PA-5250 spełniających poniższe parametry techniczne (urządzenia będą działać w dwóch klastrach):
    - 2.1.1. zaporą rdzenia PA-5250 wraz z zasilaczami AC - łącznie 2 sztuki,
    - 2.1.2. po 16 modułów 10GE SFP+ SR na każde urządzenie – łącznie 32 sztuk,
    - 2.1.3. po 4 moduły 10GE SFP+ SR dedykowanych dla przełączników HP 12910 FlexFabric (muszą być wspierane i kompatybilne z wymienionym urządzeniem) – łącznie 8 sztuk,
    - 2.1.4. 3 letnie licencje Threat prevention na każde urządzenie – łącznie 2 sztuki,
    - 2.1.5. 3 letnie licencje URL Filtering na każde urządzenie – łącznie 2 sztuki,
    - 2.1.6. 3 letnie licencje DNS Security na każde urządzenie – łącznie 2 sztuki,
    - 2.1.7. 3 letni support (Usługę Opieki Serwisowej) na każde urządzenie – łącznie 2 sztuki.

Zamawiający wymaga:
  - 2.2. Aby wszystkie powyżej wskazane elementy (pkt. 2.1.1. – 2.1.7.) pochodziły od producenta posiadanego rozwiązania – Palo Alto.
  - 2.3. Dostarczenia urządzeń z 36 miesięczną gwarancją producenta.
  - 2.4. Wykonania Wdrożenia Sprzętu IT, zgodnie z zasadami określonymi w ppu wraz z załącznikami, stanowiącymi załącznik nr 7 do SWZ.
  - 2.5. Wykonania Projektu technicznego i Dokumentacji powykonawczej w formie elektronicznej;
  - 2.6. Świadczenia Serwisu gwarancyjnego dla Sprzętu IT (wraz ze wsparciem producenta), z czasem naprawy 6 godzin, przez okres 36 miesięcy na warunkach opisanych w ppu, stanowiących załącznik nr 7 do SWZ;
  - 2.7. Oprogramowanie każdego z urządzeń realizujące wszystkie wymagane funkcje, jak też samo urządzenie musi być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowania np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania. Wszystkie funkcjonalności muszą być opublikowane na stronie producenta na dzień składania oferty.
  - 2.8. Dostarczone urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, posiadać oznaczenie CE (zgodność z dyrektywami UE) oraz zapewniać gwarancję producenta dla użytkowników z obszaru Rzeczypospolitej Polskiej.
  - 2.9. Aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia w okresie obowiązywania serwisu gwarancyjnego (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne).
  - 2.10. Zamawiający wymaga oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie będą naruszały istniejącej gwarancji dla posiadanych urządzeń i Oprogramowania.
  - 2.11. Zamawiający wymaga oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie naruszają istniejącej gwarancji oraz pochodzą z autoryzowanego kanału sprzedaży na rynek Polski.
  - 2.12. Zapewnienie przez Wykonawcę do 300 godzin konsultacji technicznych w okresie trwania Serwisu gwarancyjnego, jednak nie mniej niż 150 godzin. Konsultacje będą obejmowały analizy, audyty oraz rekomendacje 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.
  - 2.13. W ramach konsultacji technicznych Wykonawca na wniosek Zamawiającego przeprowadzi warsztaty lub prezentacje dotyczące wskazanego elementu Sprzętu IT lub Oprogramowania w Centrali Zamawiającego przy ul. Poleczki 33 w Warszawie. Czas dojazdu do Zamawiającego nie będzie wliczony jako wykorzystanie dostępnej puli godzin. Zamawiający dopuszcza przeprowadzenie konsultacji w formie zdalnej. Decyzję o formie przeprowadzenia konsultacji każdorazowo podejmie Zamawiający.

3. Zamawiający dopuszcza zaferowanie rozwiązania równoważnego poprzez dostarczenie urządzeń zgodnych ze specyfikacją zawartą w Tabeli 1 oraz Tabeli 2 zamieszczonych w pkt 4 poniżej. W przypadku zaferowania rozwiązania równoważnego Zamawiający wymaga spełnienia następujących wymagań:
- 3.1. dostarczenie 4 urządzeń zgodnych z wymaganiami zawartymi w Tabeli 1 zamieszczonej w pkt 4 poniżej.
  - 3.2. dostarczenie systemu zarządzania opisanego w Tabeli 2 zamieszczonej w pkt 4 poniżej.
  - 3.3. dostarczenie licencji i Serwisu gwarancyjnego na 3 lata od odebrania dokumentacji powykonawczej.
  - 3.4. uruchomienie i wdrożenie przez Wykonawcę zapór rdzenia oraz przeniesie na nie polityki z eksploatowanych obecnie przez Zamawiającego zapór rdzenia (składającego się z dwóch klastrów Check Point oraz z klastra Palo Alto - po dwa urządzenia w klastrze):
    - 3.1.1. proces wdrażania firewalli nie może spowodować przerwy dłuższej niż 2 godziny,
    - 3.1.2. wdrożenie musi się odbyć w przerwie serwisowej, której datę i godzinę wskaże Zamawiający na etapie uzgodnień z Wykonawcą.
  - 3.5. uruchomienie i wdrożenie przez Wykonawcę Oprogramowania dla zapór rdzenia oraz przeniesie polityki, obiekty, logi (bezsstratnie) z eksploatowanego obecnie przez Zamawiającego systemu Panorama:
    - 3.5.1. proces wdrażania systemu zarządzania nie może spowodować utraty logów,
    - 3.5.2. wdrożenie musi się odbyć w przerwie serwisowej, której datę i godzinę wskaże Zamawiający na etapie uzgodnień z Wykonawcą,
  - 3.6. W przypadku zaferowania przez Wykonawcę rozwiązania równoważnego, Zamawiający wymaga dostarczenia wraz z ofertą kopii dokumentacji oferowanego systemu, publikowanej na ogólnie dostępnych stronach internetowych producenta, w której Wykonawca zaznaczy fragmenty wskazujące spełnienie poszczególnych wymagań równoważnych opisanych w tabelach 1 i 2. Muszą to być odwołania wprost do poszczególnych wymagań SWZ. Dokumentacja ta musi być w języku polskim. W przypadku, gdy producent na swoich stronach internetowych nie publikuje dokumentacji w języku polskim, Wykonawca dokona tłumaczenia język polski. Za prawidłowość tłumaczenia odpowiada Wykonawca.
4. Zamawiający poniżej przedstawia wymagania równoważne dotyczące jednego urządzenia (poza wymaganiem Clientless VPN określonym w pkt. 11 w tabeli 1). Urządzenia będą działać w klastrze HA.

Tabela 1 - Minimalne wymagania równoważności dla urządzenia.

Nr	Wymagania minimalne
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". Wysokość maksymalnie 3U. Całość sprzętu musi być zarządzana przez jednego producenta.
2	Urządzenie musi być wyposażone w <ol style="list-style-type: none"> <li>1. 4 interfejsy 100/1000 Ethernet (RJ45)</li> <li>2. 16 interfejsów 1/10GE SFP+ obsadzone modułami 10GE SFP+ SR</li> <li>3. 4 porty 40GE/100GE QSFP+</li> </ol> UWAGA – wszystkie moduły (ilości) SFP/QSFP są podane dla jednego urządzenia
3	Urządzenie musi być wyposażone w dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w moduł Lights Out Management (LOM) lub odpowiednik pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania)
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: <ol style="list-style-type: none"> <li>1. Minimum 35 Gbps dla Firewall/kontroli aplikacji.</li> <li>2. Minimum 24 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware.</li> <li>3. Minimum 350 000 nowych połączeń na sekundę.</li> <li>4. Minimum 8 000 000 równoległych sesji.</li> </ol> <p>Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.</p> <p>Jako scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.</p>

5	<p>Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy</p> <ol style="list-style-type: none"> <li>1. rutera (tzn. w warstwie 3 modelu OSI),</li> <li>2. przełącznika (tzn. w warstwie 2 modelu OSI),</li> <li>3. w trybie pasywnego nasłuchu (sniffer).</li> </ol>
6	<p>Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)</p>
7	<p>Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy na bazie, których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.</p>
8	<p>Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.</p>
9	<p>Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPsec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi, dla zapewnienia poufności i integralności danych, wykorzystywać TLS i IPsec..</p>
10	<p>Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:</p> <ol style="list-style-type: none"> <li>1. Minimum 18 Gbps dla IPSEC VPN.</li> <li>2. Minimum 4 000 tuneli IPSEC VPN (site-to-site).</li> <li>3. Minimum 30 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, Linux, MacOS, Android, iOS.</li> <li>4. Minimum 2 000 tuneli tzw. Clientless VPN - bez konieczności zastosowania klienta VPN.</li> </ol>
11	<p>Funkcjonalność Clientless VPN, klienta VPN dla Linux, Android, iOS - Zamawiający wymaga dostarczenia licencji dla dwóch urządzeń w przypadku zaproponowania rozwiązania równoważnego,</p>
12	<p>Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej</p> <ol style="list-style-type: none"> <li>1. oznaczania pakietów znacznikami DiffServ,</li> <li>2. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego.</li> <li>3. utworzenia co najmniej 8 klas ruchu sieciowego.</li> <li>4. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.</li> <li>5. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego</li> </ol>
13	<p>Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.</p>
14	<p>Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.</p>
15	<p>Urządzenie musi obsługiwać nie mniej niż 100 wirtualnych routerów posiadających odrębne tabele routingu.</p>
16	<p>Urządzenie musi obsługiwać nie mniej niż 25 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 100 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:</p> <ol style="list-style-type: none"> <li>1. tablic routingu - minimum 5 per każda instancja. Jeżeli nie jest to możliwe, to dopuszcza się rozwiązania obsługujące 125 wirtualnych instancji firewall z obsługą jednej tablicy routingu per każda instancja.</li> <li>2. Polityk bezpieczeństwa obejmujących: <ol style="list-style-type: none"> <li>1) System IPS</li> <li>2) System ochrony antymalware/antyspyware</li> <li>3) System ochrony antywirus</li> </ol> </li> <li>3. Koncentratorów VPN dla zdalnego dostępu</li> </ol>
17	<p>Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.</p>
18	<p>Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.</p>
19	<p>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. Urządzenie musi</p>

	umożliwić zdefiniowanie nie mniej niż 60 000 reguł polityki bezpieczeństwa oraz obsługę minimum 15 000 stref bezpieczeństwa.
20	<p>Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.</p> <p>Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.</p>
21	Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość” w polityce.
22	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
23	Urządzenie musi umożliwiać budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory, kondycja bezpieczeństwa stacji końcowej
24	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. Funkcja realizowana za pomocą profilu w ramach reguł bezpieczeństwa.
25	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
26	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download”.
27	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębszej inspekcji rozdzielny od polityk bezpieczeństwa. Deszyfracja ruchu SSL będzie realizowana przed politykami bezpieczeństwa.
28	Urządzenie musi posiadać funkcję deszyfrowania ruchu TLS 1.2 i TLS 1.3 oraz wspierać protokół HTTP/2.
29	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
30	<p>Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:</p> <ol style="list-style-type: none"> <li>1. Microsoft Active Directory,</li> <li>2. usługi katalogowe LDAP,</li> <li>3. serwery Terminal Services,</li> <li>4. logi z syslog.</li> </ol>
31	<p>Urządzenie musi umożliwiać ustalić tożsamość użytkownika firewall poprzez aktywne uwierzytelnienie użytkownika z wykorzystaniem przeglądarki i captive portalu. Musi istnieć możliwość zdefiniowania co najmniej następujących rodzajów baz użytkowników dla captive portalu:</p> <ol style="list-style-type: none"> <li>1. lokalna baza danych utrzymywana na firewallu.</li> <li>2. zewnętrzna usługa katalogowa dostępna po LDAPS.</li> <li>3. zewnętrzna usługa uwierzytelnienia i autoryzacji po RADIUS.</li> </ol> <p>Captive portal musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.</p>
32	Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet, gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
33	<p>Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji.</p> <p>System IPS musi działać w warstwie 7 modelu OSI.</p>



	<p>Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia.</p> <p>Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa)</p> <p>Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi czy wsparcia producenta.</p> <p>Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
34	<p>Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji.</p> <p>Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekodery taki jak http, smtp, imap, pop3, ftp, smb.</p> <p>Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń</p> <p>Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).</p> <p>Moduł AV musi wspierać protokół http/2.</p> <p>Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
35	<p>Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware.</p> <p>Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p> <p>Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).</p> <p>Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.</p> <p>Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
36	<p>Urządzenie NGFW musi umożliwiać granularną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa – nie dopuszcza się by IPS /lub AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego.</p>
37	<p>Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).</p> <p>Ochrona DNS co najmniej w zakresie</p> <ol style="list-style-type: none"> <li>1. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA).</li> <li>2. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych.</li> <li>3. wykrywanie domen dynamicznych Dynamic DNS.</li> <li>4. wykrywanie zapytań do domen złośliwych, baza domen złośliwych musi posiadać co najmniej 10 milionów rekordów.</li> <li>5. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing).</li> </ol> <p>Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
38	<p>Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.</p>
39	<p>Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering.</p> <p>Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL.</p> <p>Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).</p>

	<p>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.</p> <p>Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
40	Urządzenie musi posiadać funkcję ochrony przed atakami typu Zero-Day na bazie współpracy ze środowiskiem typu Sandbox. Wymagane jest, aby system pozwalał na przesyłanie do systemu Sandbox co najmniej plików wykonywalnych.
41	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
42	<p>1. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:</p> <p>1.1. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu.</p> <p>1.2. Operator, który ma możliwość tylko odczytu konfiguracji.</p> <p>2. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą</p> <p>2.1. bazy lokalnej,</p> <p>2.2. serwera LDAPS,</p> <p>2.3. RADIUS lub TACACS+</p> <p>2.4. SAML 2,0</p> <p>Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).</p>
43	Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
44	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
45	Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych. W szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
46	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. Musi istnieć możliwość przekierowania logowania różnych polityk bezpieczeństwa do różnych serwerów SYSLOG.
47	Urządzenie musi obsługiwać funkcjonalność typu Netflow, sFlow, jFlow itp.
48	Urządzenie musi być wyposażone w zasilacze typu AC Hot-Swap pracujące redundantnie.
49	Urządzenie musi być wyposażone w lokalną przestrzeń na logi o pojemności 2TB (przebieg użyteczna) działającej w RAID1
50	Urządzenie musi zostać dostarczone z 36 miesięczną gwarancją producenta.
51	Oprogramowanie każdego z urządzeń realizujące wszystkie wymagane funkcje jak też samo urządzenie musi być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania Wszystkie funkcjonalności muszą być opublikowane na stronie producenta na dzień składania oferty.
52	Dostarczone urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, posiadać oznaczenie CE (zgodność z dyrektywami UE) oraz zapewniać gwarancję producenta dla użytkowników z obszaru Rzeczypospolitej Polskiej.  Zamawiający wymaga oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie będą naruszały istniejącej gwarancji dla posiadanych urządzeń i Oprogramowania.

53	Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia w najbliższym czasie (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne).
----	---

Tabela .2 – Minimalne wymagania równoważne dotyczące jednego systemu zarządzania.

Nr	Wymagania minimalne
1	Wraz z urządzeniami zapór rdzenia konieczne jest dostarczenie centralnego systemu zarządzania dostarczonego wraz z wszystkimi niezbędnymi elementami np. serwery, systemy operacyjne, systemy wirtualizacji
2	Urządzenia, na których będzie uruchomiony system zarządzania, logowania i raportowania, muszą spełniać co najmniej poniżej wskazane parametry tj.: 1. 16 CPU 2. 32 GB RAM 3. 24 TB przestrzeni dyskowej
3	System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne 1. obsługa nie mniej niż 20 firewalli fizycznych 2. obsługa nie mniej niż 1200 firewalli wirtualnych (w rozumieniu wirtualny kontekst/domena/system uruchomiony na dostarczonym firewallu) 3. obsługa co najmniej 10 000 logów/zdarzeń na sekundę 4. obsługa co najmniej 24 TB użytecznej przestrzeni dyskowej na logi
4	System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. 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 co najmniej 1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 2. tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. 3. tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych zapór rdzenia. 4. 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. 5. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”
6	System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej: 1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. >> Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) >> 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 firewalles w jednym, centralnym repozytorium. 5. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 6. Zarządzanie obiektami używanymi przez wszystkie firewalles w jednym, centralnym repozytorium 7. 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 co najmniej 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 urzędu lub grupy urzędów/logicznych systemów.
9	Dostarczane zapory rdzenia, zapory brzegowe oraz system zarządzania muszą pochodzić od jednego producenta
10	System zarządzania, logowania i raportowania musi zostać dostarczony z 36 miesięcznym Serwisem gwarancyjnym.

**Wszystkie elementy opisane w Tabeli nr 1- Minimalne wymagania równoważności dla urzędu oraz w Tabeli nr 2 – Minimalne wymagania równoważne dotyczące jednego systemu zarządzania muszą pochodzić od producenta oferowanego rozwiązania.**

16. Zamawiający wymaga, aby wykonanie przedmiotu zamówienia nastąpiło na warunkach i zasadach określonych w ppu wraz z załącznikami, stanowiących Załącznik nr 7 do SWZ.

#### **I.2. Opis części zamówienia**

1. Zamawiający nie dopuszcza składania przez Wykonawców ofert częściowych w rozumieniu art. 7 pkt 15) ustawy.
2. Zamawiający wskazuje powody niedokonania podziału zamówienia na części.  
Oprogramowanie wraz z platformą sprzętową będące przedmiotem zamówienia są kluczowymi elementami obsługującymi dostęp do internetu za pomocą klastra firewall-i (zapór ogniowych) w Agencji. Biorąc pod uwagę ten fakt, celem jaki Zamawiający chce osiągnąć poprzez udzielenie zamówienia jest sprawne działanie klastra firewall-i (zapór ogniowych) jako całości (platforma sprzętowa i oprogramowanie). Podział przedmiotowego zamówienia na części nie jest zasadny. Podział zamówienia mógłby doprowadzić do konieczności koordynacji dwóch Wykonawców, co może znacząco utrudnić, a w skrajnych przypadkach uniemożliwić sprawne działanie klastra firewall-i (zapór ogniowych) w ARiMR jako całości. W przypadku podziału zamówienia skuteczne usuwanie awarii oraz wyegzekwowanie należności odszkodowawczej ze względu na brak możliwości udowodnienia winy, która stanowiłaby podstawę naliczenia ewentualnych kar umownych mógłby być utrudniony. W przypadku podziału zamówienia na części skoordynowanie działań różnych Wykonawców realizujących poszczególne części zamówienia mogłoby poważnie zagrozić właściwemu wykonaniu zamówienia, np. w skrajnym przypadku uchylanie się od odpowiedzialności za nieprawidłowe działanie systemu jako całości zarówno przez Wykonawcę odpowiedzialnego za wsparcie oprogramowania, jak i przez Wykonawcę realizującego wsparcie dla platformy sprzętowej. Platformę sprzętową i oprogramowanie systemu klastra firewall-i (zapór ogniowych) należy traktować jako jednorodne środowisko i rozwiązanie, które gwarantuje jego bezawaryjną pracę jako całości systemu pod względem sprawności działania i bezpieczeństwa. W związku z powyższym nie ma możliwości dzielenia zamówienia na części np. na platformę sprzętową i osobno na oprogramowanie.

#### **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, jeżeli są już znani.

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

1. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 8 ustawy.
2. Zamawiający nie dopuszcza składania ofert wariantowych w rozumieniu ustawy.
3. Zamawiający nie przewiduje zawarcia umowy ramowej, 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**

1. Zamawiający wymaga realizacji zamówienia tj. dostarczenia Sprzętu IT oraz Oprogramowania, Dokumentów oraz Wdrożenia w Centralnych Ośrodkach Przetwarzania Danych (COPD) nie później niż w terminie do 45 Dni Roboczych od dnia zawarcia Umowy.
2. Serwis gwarancyjny świadczony będzie przez Wykonawcę przez okres 36 miesięcy od dnia podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w §4 ust. 10 ppu stanowiących Załącznik nr 7 do SWZ.
3. Szczegółowe terminy realizacji zobowiązań umownych zostały określone przez Zamawiającego w ppu stanowiących Załącznik nr 7 do SWZ.

#### **Rozdział III. Podstawy wykluczenia oraz warunki udziału w postępowaniu, jednolity europejski dokument zamówienia**

1. O zamówienie objęte niniejszym postępowaniem mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu z postępowania na podstawie przesłanek wskazanych w Rozdz. III.1. SWZ oraz spełniają warunki udziału w postępowaniu opisane w Rozdz. III.2. SWZ.
2. Wykonawca jest zobowiązany wykazać, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z postępowania. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia brak podstaw wykluczenia, o których mowa w Rozdz. III.1. SWZ musi wykazać każdy Wykonawca z osobna.

3. Zamawiający informuje, że zgodnie z procedurą wskazaną w art. 139 ust. 1 ustawy, najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej Wykonawcy, którego oferta została najwyższej oceniona (na podstawie kryteriów oceny ofert określonych w SWZ) w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.

### III.1. Podstawy wykluczenia

1. Z postępowania, na podstawie art. 108 ust. 1 ustawy, Zamawiający wykluczy Wykonawcę:
  - 1.1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
    - 1.1.1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
    - 1.1.2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
    - 1.1.3. o którym mowa w art. 228-230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
    - 1.1.4. finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
    - 1.1.5. o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
    - 1.1.6. powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,
    - 1.1.7. przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
    - 1.1.8. o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
  - 1.2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, współnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1.1.;
  - 1.3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
  - 1.4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
  - 1.5. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
  - 1.6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z Wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
2. Z postępowania, na podstawie art. 109 ust. 1, Zamawiający wykluczy Wykonawcę:
  - 2.1. który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3 ustawy, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert 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;
  - 2.2. który naruszył obowiązki w dziedzinie ochrony środowiska, prawa socjalnego lub prawa pracy:
    - 2.2.1. będącego osobą fizyczną skazanego prawomocnie za przestępstwo przeciwko środowisku, o którym mowa w rozdziale XXII Kodeksu karnego lub za przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, o którym mowa w rozdziale XXVIII Kodeksu karnego, lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego,
    - 2.2.2. będącego osobą fizyczną prawomocnie ukaranego za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny,
    - 2.2.3. wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z prawa ochrony środowiska, prawa pracy lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną;

- 2.3. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, współnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo lub ukarano za wykroczenie, o którym mowa w art. 109 pkt 2 lit. a) lub b) ustawy.
- 2.4. w stosunku, do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
- 2.5. 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 dowodów;
- 2.6. jeżeli występuje konflikt interesów w rozumieniu art. 56 ust. 2 ustawy, którego nie można skutecznie wyeliminować w inny sposób niż przez wykluczenie Wykonawcy;
- 2.7. który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;
- 2.8. który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
- 2.9. który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
- 2.10. który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia.

### III.2. Warunki udziału w postępowaniu

1. O niniejsze zamówienie mogą ubiegać się Wykonawcy spełniający warunki udziału w postępowaniu w zakresie:
  - 1.1. **Zdolności technicznej lub zawodowej.** Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że:
    - 1.1.1. wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, a w przypadku świadczeń okresowych lub ciągłych również realizuje: co najmniej 2 (dwie) usługi polegające na dostarczeniu, zainstalowaniu i produkcyjnym uruchomieniu urządzeń typu firewall (urządzenia pełniące funkcje zapory ogniowej) o wartości każdej z nich nie mniejszej niż 700 000,00 zł brutto (słownie: siedemset tysięcy złotych, 00/100).

#### UWAGA 1

*Jeżeli wartość usługi 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](http://www.nbp.pl) tabela A – tabela kursów średnich walut obcych) z dnia zakończenia usługi 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 usług nadal realizowanych - wg tabeli kursów średnich walut obcych z dnia rozpoczęcia realizacji danej usługi.*

- 1.1.2. 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:**
  - 1.1.2.1. co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.1.1. z wyłączeniem wartości zamówień;
  - 1.1.2.2. certyfikat PCNSE Palo Alto Networks Certified Network Security Engineer 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:
  - a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,
  - b) analogiczny stopień poziomu kompetencji,
  - c) 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 odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonują usługi, do realizacji których te*

*zdolności są wymagane. W takiej sytuacji Wykonawca składa wraz z ofertą oświadczenie w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 4 do SWZ.*

2. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w Rozdz. IV niniejszej SWZ. Z treści złożonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.

#### **Rozdział IV. Zawartość ofert, wykaz podmiotowych środków dowodowych**

1. W zakresie nieuregulowanym postanowieniami SWZ zastosowanie mają przepisy rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie rodzajów podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415; dalej: „*Rozporządzenie w sprawie rodzajów podmiotowych środków dowodowych*”).
2. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w terminie przez siebie wskazanym, chyba że:
  - 2.1. oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub
  - 2.2. zachodzą przesłanki unieważnienia postępowania.

##### **IV.1. Zawartość ofert**

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej, podpisaną kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym wg Załącznika nr 1 albo 1A do SWZ za pośrednictwem Platformy Zakupowej.
2. Wykonawca obowiązany jest złożyć wraz z ofertą następujące dokumenty oraz przedmiotowe środki dowodowe:
  - 2.1. Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu Wykonawcy jest umocowana do jego reprezentowania.
  - 2.2. Pełnomocnictwo lub inny dokument potwierdzający umocowanie osoby działającej w imieniu Wykonawcy do jego reprezentowania, jeżeli oferta nie została podpisana przez osoby upoważnione do tych czynności dokumentem rejestracyjnym.
  - 2.3. Dowód wniesienia wadium. Jeżeli Wykonawca wnosi wadium w formie gwarancji lub poręczenia Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej. W przypadku wniesienia wadium w innej formie niż pieniądź, powinno ono obowiązywać przez cały okres związania ofertą.
  - 2.4. Zobowiązanie podmiotów udostępniających zasoby do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie będzie dysponował niezbędnymi zasobami, jeżeli Wykonawca powołuje się na zasoby innych podmiotów. Zobowiązanie winno być podpisane przez osobę upoważnioną do reprezentacji podmiotu udostępniającego zasoby. Zapisy pkt 2.1. i 2.2. oraz Rozdz. IV.5 SWZ stosuje się odpowiednio.
  - 2.5. 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 (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16). Dokument JEDZ należy złożyć pod rygorem nieważności w formie elektronicznej. Dokument JEDZ musi być opatrzony kwalifikowanym podpisem elektronicznym.
  - 2.6. Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia w zakresie wskazania, które usługi wykonają poszczególni Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (członkowie konsorcjum). Wzór oświadczenia stanowi Załącznik nr 4 do SWZ.
  - 2.7. W celu potwierdzenia zgodności oferowanych urządzeń z wymaganiami określonymi w opisie przedmiotu zamówienia, Zamawiający żąda złożenia następujących przedmiotowych środków dowodowych:
    - 2.7.1. Kopii dokumentacji oferowanego systemu, publikowanej na ogólnie dostępnych stronach internetowych Producenta, w której Wykonawca zaznaczy fragmenty wskazujące spełnienie poszczególnych wymagań równoważnych opisanych w Tabelach 1 i 2 (minimalne parametry równoważności dla urządzeń oraz systemu zarządzania),
    - 2.7.2. Oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie naruszają istniejącej gwarancji (dotyczy rozwiązania opisanego w rozdz. I.1 pkt 2.1. SWZ) oraz pochodzą z autoryzowanego kanału sprzedaży na rynek polski.
    - 2.7.3. Oświadczenie Wykonawcy, że urządzenia będą dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia w okresie obowiązywania serwisu gwarancyjnego (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne).

**UWAGA:** Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie, chyba że pomimo złożenia przedmiotowego środka dowodowego oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia.

#### 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 udostępni Wykonawcom plik, w formacie XML, wygenerowany z narzędzia ESPD, który stanowi Załącznik nr 8 do SWZ.
  - 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. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie JEDZ, o którym mowa w Rozdz. IV.1. pkt 2.5. SWZ, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia także oświadczenie JEDZ, o którym mowa w Rozdz. IV.1. pkt 2.5. SWZ podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.
4. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez Wykonawcę, jest Platforma Zakupowa.
5. Dokument elektroniczny JEDZ należy złożyć w formacie PDF.
6. Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 128 ust. 1 ustawy.

#### IV.3. Wykaz podmiotowych środków dowodowych

Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia za pośrednictwem Platformy Zakupowej, w wyznaczonym terminie, nie krótszym niż 10 dni od dnia wezwania, aktualnych na dzień złożenia podmiotowych środków dowodowych, w formie elektronicznej podpisanych kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności, w poniższym zakresie:

1. braku podstaw wykluczenia Wykonawcy z postępowania o udzielenie zamówienia:
  - 1.1. informacji z Krajowego Rejestru Karnego w zakresie:
    - 1.1.1. art. 108 ust. 1 pkt 1 i 2 ustawy,
    - 1.1.2. art. 108 ust. 1 pkt 4 ustawy, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,
    - 1.1.3. art. 109 ust. 1 pkt 2 lit. a ustawy,
    - 1.1.4. art. 109 ust. 1 pkt 2 lit. b ustawy, dotyczącej ukarania za wykroczenie, za które wymierzono karę aresztu,
    - 1.1.5. art. 109 ust. 1 pkt 3 ustawy, dotyczącej skazania za przestępstwo lub ukarania za wykroczenie, za które wymierzono karę aresztu
 - sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;
  - 1.2. zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków i opłat, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem podatków lub opłat wraz z zaświadczeniem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert Wykonawca dokonał płatności należnych podatków lub opłat wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
  - 1.3. zaświadczenia albo innego dokumentu właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub właściwego oddziału regionalnego lub właściwej placówki terenowej Kasy Rolniczego Ubezpieczenia Społecznego potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne, w zakresie art. 109 ust. 1 pkt 1 ustawy, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne wraz z zaświadczeniem albo innym dokumentem zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert Wykonawca dokonał płatności należnych składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
  - 1.4. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
  - 1.5. oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:
    - 1.5.1. art. 108 ust. 1 pkt 3 ustawy,
    - 1.5.2. art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
    - 1.5.3. art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
    - 1.5.4. art. 108 ust. 1 pkt 6 ustawy,



- 1.5.5. art. 109 ust. 1 pkt 1 ustawy, odnośnie do naruszenia obowiązków dotyczących płatności podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2019 r. poz. 1170 z późn. zm.),
- 1.5.6. art. 109 ust. 1 pkt 2 lit. b ustawy, dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,
- 1.5.7. art. 109 ust. 1 pkt 2 lit. c ustawy,
- 1.5.8. art. 109 ust. 1 pkt 3 ustawy, dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,
- 1.5.9. art. 109 ust. 1 pkt 5-10 ustawy  
- sporządzone według wzoru, który stanowi załącznik nr 2 do SWZ.
- 1.6. oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. Wzór oświadczenia stanowi Załącznik nr 3 do SWZ.
- 2. potwierdzenia spełnienia warunków udziału w postępowaniu dotyczących zdolności zawodowej:
  - 2.1. wykazu usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy. Wzór oświadczenia stanowi Załącznik nr 5 do SWZ.
  - 2.2. wykazu osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia 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 6 do SWZ.

#### **IV.4. Podmiotowe środki dowodowe składane przez Wykonawców mających siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej**

- 1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast:
  - 1.1. informacji z Krajowego Rejestru Karnego, o której mowa w Rozdz. IV.3 pkt 1.1. SWZ – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, w zakresie, o którym mowa w Rozdz. IV.3 pkt 1.1. SWZ;
  - 1.2. zaświadczenia, o którym mowa w Rozdz. IV.3 pkt 1.2. SWZ, zaświadczenia albo innego dokumentu potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, o których mowa w Rozdz. IV.3 pkt 1.3 SWZ, lub odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w Rozdz. IV.3 pkt 1.4. SWZ – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
    - 1.2.1. nie naruszył obowiązków dotyczących płatności podatków, opłat, lub składek na ubezpieczenie społeczne lub zdrowotne,
    - 1.2.2. nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
- 2. Dokument, o którym mowa w pkt 1.1., powinien być wystawiony nie wcześniej niż 6 miesięcy przed ich złożeniem. Dokumenty, o którym mowa w pkt 1.2., powinny być wystawione nie wcześniej niż 3 miesiące przed jego złożeniem.
- 3. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt. 1, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4, art. 109 ust. 1 pkt 1, 2 lit. a i b oraz pkt 3 ustawy, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Postanowienie pkt. 2 stosuje się.

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

- 1. Wykonawca może w celu potwierdzenia spełnienia warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

2. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających **zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby** do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
3. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w pkt 2, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
  - 1.1. zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
  - 1.2. sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
  - 1.3. czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.
4. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.
5. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 ustawy, przedstawienia w odniesieniu do tych podmiotów podmiotowych środków dowodowych wymienionych w Rozdz. IV.3 pkt 1.1. – 1.5. SWZ. Postanowienia Rozdz. IV.3. SWZ stosuje się odpowiednio.

#### IV.6. Klauzule informacyjne w zakresie 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” Zamawiający informuje, że:

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 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: [info@arimr.gov.pl](mailto:info@arimr.gov.pl) lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
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](mailto:iod@arimr.gov.pl) lub pisemnie na adres korespondencyjny Administratora, wskazanych w pkt 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.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
  - 4.1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 2 ustawy,
  - 4.2. organy kontrolne,
  - 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. z 2020 r. poz. 2176),
  - 4.4. podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa.
5. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia niniejszego postępowania. Ponadto, zgodnie z art. 78 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.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania oraz prawo żądania ograniczenia przetwarzania 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. 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 komunikowania 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 albo postaci elektronicznej, w zależności od rodzaju przekazywanego dokumentu – stosownie do obowiązujących w tym zakresie przepisów prawa. 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.2610.10.2021**, Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wskazany numer referencyjny.

3. Wykonawcy powinni kierować do Zamawiającego wszelką korespondencję z zachowaniem zasad opisanych w pkt 1, za pośrednictwem Platformy Zakupowej.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ. Wniosek należy przesłać za pośrednictwem Platformy Zakupowej.
5. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 14 dni przed upływem terminu składania ofert. Treść pytań (bez ujawnienia źródła zapytania) wraz z wyjaśnieniami bądź informacje o dokonaniu zmiany treści SWZ, Zamawiający przekaże (opublikuje) Wykonawcom za pośrednictwem Platformy Zakupowej.
6. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego po upływie terminu, o którym mowa w pkt 5 Zamawiający nie ma obowiązku udzielania wyjaśnień treści SWZ.
7. W uzasadnionym przypadku Zamawiający może przed terminem składania ofert zmienić treść dokumentów składających się na niniejszą SWZ.
8. Zamawiający nie zamierza zwoływać zebrania Wykonawców.
9. Osobami uprawnionymi ze strony Zamawiającego do kontaktów z Wykonawcami są:
  - 9.1. Pani Agnieszka Skarzyńska, tel. +48225950065 w godz. 9.00 – 15.00.
  - 9.2. Pan Zbigniew Antonik, tel.: +48225950062 w godz. 9.00 – 15.00.

## Rozdział VI. Wymagania dotyczące wadium

1. Wykonawca zobowiązany jest wnieść wadium w wysokości **42 000,00 zł** (słownie: czterdzieści dwa tysiące złotych 00/100).
2. Wadium może być wniesione w:
  - 2.1. pieniądzu
  - 2.2. gwarancjach bankowych;
  - 2.3. gwarancjach ubezpieczeniowych;
  - 2.4. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2020 r. poz. 299).
3. Wadium w formie pieniądza należy wnieść przelewem na rachunek bankowy Zamawiającego prowadzony 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 Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami”.
4. W przypadku wnoszenia wadium w formie gwarancji lub poręczenia, o których mowa w pkt. 2.2.-2.4., Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej poprzez wczytanie na Platformie Zakupowej. Wadium powinno być oznaczone w następujący sposób: **WADIUM – numer referencyjny sprawy, nazwa postępowania lub w inny sposób umożliwiający identyfikację postępowania, którego dotyczy.**
5. Dokument wadialny (gwarancja lub poręczenie) musi wyraźnie wskazywać na wszystkie okoliczności jego utraty określone w art. 98 ust. 6 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. 98 ust. 6 ustawy.
7. Oferta Wykonawcy, który nie wniósł wadium lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 ustawy 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 90 dni tj. do dnia **19.02.2022 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

## Rozdział VIII Opis sposobu przygotowywania ofert

### VIII.1. Przygotowanie ofert

1. Ofertę wraz z przedmiotowymi środkami dowodowymi należy złożyć pod rygorem nieważności w formie elektronicznej. Ofertę należy podpisać kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Wykonawca składa ofertę na Formularzu Ofertowym (wg Załącznika nr 1 albo 1A do SWZ).
2. Treść złożonej oferty musi być zgodna z warunkami zamówienia. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferta powinna być sporządzona w języku polskim, w formie elektronicznej pod rygorem nieważności. Ofertę należy podpisać kwalifikowanym podpisem elektronicznym. Ofertę należy złożyć 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. 74 ust. 1 i 2 ustawy oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu niezwłocznie po otwarciu ofert, 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. 222 ust. 5 ustawy, tj. nazw albo imion i nazwisk oraz siedzib lub miejsc prowadzonej działalności gospodarczej albo miejsc zamieszkania Wykonawców, których oferty zostały otwarte, cen lub kosztów zawartych w ofertach.

**Uwaga:**

*Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), które Wykonawca zamierza zastrzec jako tajemnicę przedsiębiorstwa, muszą zostać odpowiednio oznaczone a następnie 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 przesłanek określonych w Rozdz. III.1. SWZ,
  - 6.3. zgodnie z art. 58 ust. 2 ustawy muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie 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,
  - 6.6. w odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonują usługi, do realizacji których te zdolności są wymagane.

**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 (tj. Dz. U. z 2020 r. poz. 1173 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. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument.
4. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
5. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 4, dokonuje w przypadku:
  - 5.1. podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
  - 5.2. przedmiotowych środków dowodowych – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
  - 5.3. innych dokumentów, w tym dokumentów, o których mowa w art. 94 ust. 2 ustawy – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
6. Podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.
7. W przypadku gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy, oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, dokumenty, o których mowa w art. 94 ust. 2 ustawy, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu

- opatrzone kwalifikowanym podpisem elektronicznym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
8. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 7, dokonuje w przypadku:
    - 8.1. podmiotowych środków dowodowych – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
    - 8.2. przedmiotowego środka dowodowego, dokumentu, o którym mowa w art. 94 ust. 2 ustawy, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
    - 8.3. pełnomocnictwa – mocodawca.
  9. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w pkt. 4 i 7, może dokonać również notariusz.
  10. Przez cyfrowe odwzorowanie, o którym mowa w pkt. 2, 5 oraz pkt. 7-9, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiającą zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
  11. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku kwalifikowanym podpisem elektronicznym.

## **Rozdział IX. Sposób oraz termin składania i otwarcia ofert, warunki zmiany albo wycofania oferty**

### **IX.1. Sposób oraz termin składania ofert i otwarcia ofert**

1. Ofertę pod rygorem nieważności należy złożyć w formie elektronicznej. Ofertę musi zostać podpisana kwalifikowanym podpisem elektronicznym przez osoby upoważnione do tych czynności. Ofertę wraz z przedmiotowymi środkami dowodowymi należy złożyć na Platformie Zakupowej udostępnionej przez Zamawiającego na stronie internetowej: <https://platformazakupowa.pl/pn/arimr>.
2. Termin składania ofert upływa w dniu **22.11.2021 r. o godzinie 10:00**.
3. Otwarcie ofert odbędzie się w dniu **22.11.2021 r. o godzinie 11:00**.
4. Zamawiający nie bierze odpowiedzialności za nieprawidłowe złożenie oferty wynikające z niezastosowania się przez Wykonawcę do wymagań niniejszej SWZ.

### **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 nieposiadający 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 Operatora 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](mailto: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 netto, ceny ofertowej netto, należnego podatku od towarów i usług VAT oraz ceny ofertowej brutto, w sposób określony w Formularzu Ofertowym stanowiącym Załącznik nr 1 albo Załącznik nr 1A do SWZ (w zależności od zaferowanych urządzeń).
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 Rozdz. XIV pkt 4 niniejszej SWZ.
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 pominać, 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 dla celów zastosowania kryterium ceny lub kosztu doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. 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, wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

**Rozdział XI. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert****1.1. kryterium cena ( $P_c$ ) – waga 90% [90 pkt], wg poniższego wzoru**

$$P_c = \frac{C_{min.}}{C_b} \times 90 \text{ pkt}$$

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 4% [4 pkt], wg poniższych zasad:**

W ramach tego kryterium oferta może otrzymać łącznie nie więcej niż 4 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.	Dostarczone urządzenia będą mogły być zarządzane z posiadanej przez Zamawiającego konsoli Panorama i współdzielić obiekty konfiguracji z posiadanymi przez Zamawiającego firewallami Palo Alto - w całościowym zakresie opisanym w wymaganiach dla systemu zarządzania. Wszystkie urządzenia firewall – zarówno posiadane przez Zamawiającego jak i dostarczone w ramach niniejszego postępowania są zarządzane z jednego centralnego systemu,	2 pkt.
2.	W przypadku utraty komunikacji z system zarządzania zaporami zapory muszą pozwalać na: <ol style="list-style-type: none"> <li>1. Lokalne zbieranie i analizowanie logów</li> <li>2. Korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:               <ol style="list-style-type: none"> <li>a. ruchu sieciowym,</li> <li>b. aplikacjach,</li> <li>c. zagrożeniach</li> <li>d. filtrowaniu stron www.</li> </ol> </li> <li>3. Tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.</li> <li>4. Tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.</li> </ol>	1 pkt.
3.	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzania zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami oraz możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. Realizacja tej funkcji musi odbywać się w oparciu o sam firewall.	1 pkt.

**Uwagi:**

- a) 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.
- b) Wykonawca może zaoferować Sprzęt IT spełniający wymagania opisane przez Zamawiającego na wszystkie ww. pozycje (tj. 3 pozycje) 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 ppu” (P<sub>D</sub>) – waga 6% [6 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	45 Dni Roboczych	0 pkt
2	44 Dni Roboczych	0,3 pkt
3	43 Dni Roboczych	0,6 pkt
4	42 Dni Roboczych	0,9 pkt
5	41 Dni Roboczych	1,2 pkt
6	40 Dni Roboczych	1,5 pkt
7	39 Dni Roboczych	1,8 pkt
8	38 Dni Roboczych	2,1 pkt
9	37 Dni Roboczych	2,4 pkt
10	36 Dni Roboczych	2,7 pkt
11	35 Dni Roboczych	3 pkt
12	34 Dni Roboczych	3,3 pkt
13	33 Dni Roboczych	3,6 pkt
14	32 Dni Roboczych	3,9 pkt
15	31 Dni Roboczych	4,2 pkt
16	30 Dni Roboczych	4,5 pkt
17	29 Dni Roboczych	4,8 pkt
18	28 Dni Roboczych	5,1 pkt
19	27 Dni Roboczych	5,4 pkt
20	26 Dni Roboczych	5,7 pkt
21	25 i mniej Dni Roboczych	6 pkt

Uwagi:

- Maksymalny termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 ppu wynosi 45 Dni Roboczych.
- Jeżeli Wykonawca zaoferuje termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 ppu dłuższy niż 45 Dni Roboczych oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z warunkami zamówienia.
- 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 ppu tj.: 45 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<sub>c</sub> – ilość punktów oferty w kryterium „Cena”;  
P<sub>T</sub> – ilość punktów oferty w kryterium „Parametry techniczne Sprzętu IT”;  
P<sub>D</sub> – 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**

- Zamawiający powiadomi wybranego Wykonawcę o miejscu i terminie podpisania umowy.
- 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**

- Zamawiający żąda od Wykonawcy, z którym zostanie podpisana umowa wniesienia zabezpieczenia należytego wykonania umowy w wysokości 2,5 % 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 Rozdz. SWZ 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” a przypadku zabezpieczenia wnoszonego w postaci elektronicznej należy przekazać na adres e-mail uzyskany od Zamawiającego przed podpisaniem umowy.
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 w projektowanych postanowieniach umowy.

#### **Rozdział XIV. Informacje dotyczące umowy w sprawie zamówienia publicznego**

1. Zawarcie umowy nastąpi wg treści projektowanych postanowień umowy w sprawie zamówienia publicznego, stanowiących Załącznik nr 7 do niniejszej SWZ.
2. Postanowienia ustalone w projektowanych postanowieniach umowy nie podlegają negocjacjom.
3. Przyjęcie niniejszych projektowanych 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 w projektowanych postanowieniach umowy wraz z załącznikami, stanowiących Załącznik nr 7 do SWZ.

#### **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 IX ustawy.
2. Odwołanie przysługuje na:
  - 2.1. niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
  - 2.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie winno zawierać informacje określone w art. 516 ust. 1 ustawy, w szczególności wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Pisma w postępowaniu odwoławczym wnosi się w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej, z tym że odwołanie i przystąpienie do postępowania odwoławczego, wniesione w postaci elektronicznej, wymagają opatrzenia podpisem zaufanym.
5. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
  - 6.1 10 (dziesięciu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej;
  - 6.2 15 (piętnastu) dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przekazane w inny sposób niż określony w pkt. 6.1.;
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie lub wobec treści dokumentów zamówienia wnosi się w terminie:



- 7.1. 10 (dziesięciu) dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej.
8. Odwołanie w przypadkach innych niż określone w pkt. 6 i 7 wnosi się w terminie:
  - 8.1. 10 (dziesięciu) dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

**Załączniki do SWZ:**

1. Załącznik nr 1 -1A- Wzór Formularza Ofertowego.
2. Załącznik nr 2 - Wzór w 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 - Oświadczenie o podziale obowiązków w trakcie realizacji zamówienia.
5. Załącznik nr 5 - Wzór Oświadczenia – Wykaz usług.
6. Załącznik nr 6 - Wzór Oświadczenia – Wykaz osób.
7. Załącznik nr 7 - projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do umowy w sprawie zamówienia publicznego
8. Załącznik nr 8 - ESPD – plik, w formacie XML, wygenerowany z narzędzia ESPD – do przygotowania formularza jednolitego europejskiego dokumentu zamówienia (JEDZ)

Zatwierdzam SWZ wraz z załącznikami:

ZASTĘPCA PREZESA



.....  
Dariusz Olkiewicz

Dariusz Olkiewicz

Zastępca Prezesa ARiMR

**Załącznik nr 1 do SWZ – wzór Formularza Ofertowego**

**Formularz Ofertowy  
DPIZP.2610.10.2021**

Ja(my) niżej podpisany(-i) .....

Działając w imieniu i na rzecz .....

.....

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na „Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami”, zgodnie z wymaganiami określonymi w specyfikacji warunków zamówienia i projektowanych postanowieniach umowy wraz z załącznikami, oferuję (-emy) realizację przedmiotu zamówienia, za cenę:

Lp.	Przedmiot	Cena jednostkowa netto zł	Ilość jedn.	Cena ofertowa netto zł	Podatek VAT*		Cena ofertowa brutto zł
					%	zł	
	a	b	c	d = b x c	e	f = d x e	g = d + f
1.	Sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem, Projektem Technicznym, Wdrożeniem i Dokumentacją powykonawczą spełniające wymagania określone w Załączniku nr 1 do ppu.  Producent ..... Model ..... * .....		2 szt.				
2.	Serwis Gwarancyjny zgodnie z § 7 ust. 1 pkt. 2) ppu		1 kpl.				
3.	Godziny konsultacji, o których mowa w § 2 ust. 4 ppu		300 godzin				
<b>Razem [Σ1+3]:</b>					<b>X</b>		

\*Zamawiający wymaga wskazania przez Wykonawcę w ofercie numeru produktów (tzw. part number) oraz nazwy wszystkich dostarczanych elementów (urządzeń, modułów, wkładek, oprogramowania w tym koniecznie wersji, itp) pozwalających je jednoznacznie zidentyfikować.

**Słownie zł cena ofertowa netto:** \_\_\_\_\_

**Słownie zł cena ofertowa brutto:** \_\_\_\_\_

## I. Wymagania dodatkowe punktowane w ramach kryterium „Parametry techniczne Sprzętu IT”

Lp.	„Parametry techniczne Sprzętu IT” (P-)	Parametr oferowany zaznacza Wykonawca
1.	Dostarczone urządzenia będą mogły być zarządzane z posiadanej przez Zamawiającego konsoli Panorama i współdzielić obiekty konfiguracji z posiadanymi przez Zamawiającego firewallami Palo Alto - w całościowym zakresie opisanym w wymaganiach dla systemu zarządzania. Wszystkie urządzenia firewall – zarówno posiadane przez Zamawiającego jak i dostarczone w ramach niniejszego postępowania są zarządzane z jednego centralnego systemu,	TAK/NIE*
2.	W przypadku utraty komunikacji z system zarządzania zaporami zapory muszą pozwalać na: <ol style="list-style-type: none"> <li>1. Lokalne zbieranie i analizowanie logów</li> <li>2. korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: <ol style="list-style-type: none"> <li>a. ruchu sieciowym,</li> <li>b. aplikacjach,</li> <li>c. zagrożeniach</li> <li>d. filtrowaniu stron www.</li> </ol> </li> <li>3. tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.</li> <li>4. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.</li> </ol>	TAK/NIE*
3.	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzeniem zmian na urządzeniu musi być możliwość przejrzania zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami oraz możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. Realizacja tej funkcji musi odbywać się w oparciu o sam firewall.	TAK/NIE*

**\* - niewłaściwe skreślić**

1. 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.
2. Wykonawca może zaoferować Sprzęt IT spełniający wymagania opisane przez Zamawiającego na wszystkie ww. pozycje (tj. 3 pozycje) 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.

**II. Wymagania dodatkowe punktowane w ramach kryterium „Dostarczenie Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy.**

1	Zgodnie z kryterium oceny ofert oferujemy Zamawiającemu <b>dostarczenie Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy w terminie ..... * Dni Roboczych</b> (Wykonawca winien wpisać liczbę Dni Roboczych <sup>1)</sup>
<p><b><sup>1)</sup> UWAGA:</b></p> <ol style="list-style-type: none"> <li>1. Maksymalny termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy wynosi 45 Dni Roboczych.</li> <li>2. Jeżeli Wykonawca zaoferuje termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy dłuższy niż 45 Dni Roboczych oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z warunkami zamówienia.</li> <li>3. 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, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy tj.: 45 Dni Roboczych.</li> </ol>	

**Oświadczamy, że:**

1. Zapoznaliśmy się z treścią specyfikacji warunków zamówienia (SWZ), w tym projektowanych postanowień umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdz. II SWZ oraz projektowanych postanowieniach umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Uważamy się za związanych niniejszą ofertą do terminu określonego w SWZ.
5. Wadium w wysokości **42 000,00 zł** (słownie: czterdzieści dwa tysiące złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
6. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku ..... Oświadczenie o zwolnieniu wadium wniesionego w innej formie niż pieniądź należy przekazać gwarantowi/poręczycielowi na następujący adres e-mail.....
7. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **2,5%** ceny całkowitej podanej w ofercie.
8. W przypadku udzielenia nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
9. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz nazwę Podwykonawcy, jeśli jest już znany):

9.1. ....<sup>1</sup>

<sup>1</sup> w przypadku niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.

10. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres e-mail: .....  
Dane kontaktowe: imię i nazwisko ....., nr tel. ...., adres e-mail: .....
11. Dokumenty wymienione od strony ..... do strony ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913) i nie mogą być ujawnione pozostałym uczestnikom postępowania.

**UWAGA:**

Zamawiający przypomina, że stosownie do treści:

- art. 18 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert **wykazać**, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa
- **Rozdz. VIII.1. pkt 5 SWZ wszelkie informacje stanowiące tajemnicę przedsiębiorstwa muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla informacji stanowiących tajemnicę przedsiębiorstwa.**

12. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)<sup>2</sup> wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.<sup>3</sup>

<sup>2</sup> 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).

<sup>3</sup> 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.).

13. Jednocześnie, zgodnie z treścią art. 225 ust. 2 ustawy oświadczam, że wybór niniejszej oferty:

13.1. **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego<sup>4</sup>

13.2. **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w związku z tym:<sup>4</sup>

13.2.1. ....<sup>5</sup>

<sup>4</sup> 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.

<sup>5</sup> W pkt. 13.2.1. należy wskazać: nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku, stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

14. Zgodnie z Rozdz. IV.1. SWZ do oferty zostają załączone dokumenty:

14.1. ....

14.2. ....

14.3. ....

14.4. ....

14.5. ....

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 1 A do SWZ – wzór Formularza Ofertowego

Formularz Ofertowy dla rozwiązania równoważnego  
DPIZP.2610.10.2021

Ja(my) niżej podpisany(-i) .....

Działając w imieniu i na rzecz .....

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na „Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami”, zgodnie z wymaganiami określonymi w specyfikacji warunków zamówienia i projektowanych postanowieniach umowy wraz z załącznikami, oferuję (-emy) realizację przedmiotu zamówienia, za cenę:

Lp.	Przedmiot	Cena jednostkowa netto zł	Ilość jedn.	Cena ofertowa netto zł	Podatek VAT*		Cena ofertowa brutto zł
					%	zł	
	a	b	c	d = b x c	e	f = d x e	g = d + f
1.	Sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem, Projektem Technicznym, Wdrożeniem i Dokumentacją powykonawczą spełniające wymagania określone w Załączniku nr 1 do ppu dla rozwiązania równoważnego.  Producent ..... Model ..... * .....		4 szt.				
2.	Serwis Gwarancyjny zgodnie z § 7 ust. 1 pkt. 2) ppu		1 kpl.				
3.	Godziny konsultacji, o których mowa w § 2 ust. 4 ppu		300 godzin				
<b>Razem [Σ1+3]:</b>					<b>X</b>		

\*Zamawiający wymaga wskazania przez Wykonawcę w ofercie numeru produktów (tzw. part number) oraz nazwy wszystkich dostarczanych elementów (urządzeń, modułów, wkładek, oprogramowania w tym koniecznie wersji, itp) pozwalających je jednoznacznie zidentyfikować.

Słownie zł cena ofertowa netto: \_\_\_\_\_

Słownie zł cena ofertowa brutto: \_\_\_\_\_

## III. Wymagania dodatkowe punktowane w ramach kryterium „Parametry techniczne Sprzętu IT”

Lp.	„Parametry techniczne Sprzętu IT” (P <sub>1</sub> )	Parametr oferowany zaznacza Wykonawca
1.	Dostarczone urządzenia będą mogły być zarządzane z posiadanej przez Zamawiającego konsoli Panorama i współdzielić obiekty konfiguracji z posiadanymi przez Zamawiającego firewallami Palo Alto - w całościowym zakresie opisanym w wymaganiach dla systemu zarządzania. Wszystkie urządzenia firewall – zarówno posiadane przez Zamawiającego jak i dostarczone w ramach niniejszego postępowania są zarządzane z jednego centralnego systemu,	TAK/NIE*
4.	W przypadku utraty komunikacji z system zarządzania zaporami zapory muszą pozwalać na: 5. Lokalne zbieranie i analizowanie logów 6. korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: e. ruchu sieciowym, f. aplikacjach, g. zagrożeniach h. filtrowaniu stron www. 7. 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. 8. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.	TAK/NIE*
5.	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzeniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami oraz możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. Realizacja tej funkcji musi odbywać się w oparciu o sam firewall.	TAK/NIE*
<p><b>* - niewłaściwe skreślić</b></p> <p>3. W przypadku <u>nie</u> przekreślenia żadnego ze zwrotów lub tęcznego przekreślenia obu zwrotów „TAK/NIE” przez Wykonawcę dla danej pozycji w Formularzu Ofertowym, Zamawiający uzna że zaofertowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.</p> <p>4. Wykonawca może zaofertować Sprzęt IT spełniający wymagania opisane przez Zamawiającego na wszystkie ww. pozycje (tj. 3 pozycje) 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.</p>		

**IV. Wymagania dodatkowe punktowane w ramach kryterium „Dostarczenie Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy.**

1	Zgodnie z kryterium oceny ofert oferujemy Zamawiającemu <b>dostarczenie Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy w terminie ..... * Dni Roboczych</b> [Wykonawca winien wpisać liczbę Dni Roboczych <sup>1)</sup>
<p><b><sup>1)</sup> UWAGA:</b></p> <p>4. <i>Maksymalny termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy wynosi 45 Dni Roboczych.</i></p> <p>5. <i>Jeżeli Wykonawca zaoferuje termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy dłuższy niż 45 Dni Roboczych oferta takiego Wykonawcy zostanie odrzucona jako niezgodna z warunkami zamówienia.</i></p> <p>6. <i>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, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy tj.: 45 Dni Roboczych.</i></p>	

**Oświadczamy, że:**

1. Zapoznaliśmy się z treścią specyfikacji warunków zamówienia (SWZ), w tym projektowanych postanowień umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte.
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdz. II SWZ oraz projektowanych postanowieniach umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Uważamy się za związanych niniejszą ofertą do terminu określonego w SWZ.
5. Wadium w wysokości **42 000,00 zł** (słownie: czterdzieści dwa tysiące złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
6. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku ..... Oświadczenie o zwolnieniu wadium wniesionego w innej formie niż pieniądz należy przekazać gwarantowi/poręczycielowi na następujący adres e-mail.....
7. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **2,5%** ceny całkowitej podanej w ofercie.
8. W przypadku udzielenia nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
9. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz nazwę Podwykonawcy, jeśli jest już znany):
  - 9.1. ....<sup>1</sup>

<sup>1</sup> w przypadku niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.
10. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres e-mail: .....  
Dane kontaktowe: imię i nazwisko ....., nr tel. ...., adres e-mail: .....
11. Dokumenty wymienione od strony ..... do strony ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913) i nie mogą być ujawnione pozostałym uczestnikom postępowania.  
**UWAGA:**  
Zamawiający przypomina, że stosownie do treści:  
– art. 18 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert **wykazać**, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa  
– **Rozdz. VIII.1. pkt 5 SWZ wszelkie informacje stanowiące tajemnicę przedsiębiorstwa muszą zostać odpowiednio oznaczone a następnie załączone na Platformie Zakupowej w osobnym pliku w miejscu właściwym dla informacji stanowiących tajemnicę przedsiębiorstwa.**
12. Wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO)<sup>2</sup> wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.<sup>3</sup>  
<sup>2</sup> 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).



<sup>3</sup> 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.).

13. Jednocześnie, zgodnie z treścią art. 225 ust. 2 ustawy oświadczam, że wybór niniejszej oferty:

13.1. nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego<sup>4</sup>

13.2. będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w związku z tym:<sup>4</sup>

13.2.1. ....<sup>5</sup>

<sup>4</sup> 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.

<sup>5</sup> W pkt. 13.2.1. należy wskazać: nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku, stawkę podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

14. Zgodnie z Rozdz. IV.1. SWZ do oferty zostają załączone dokumenty:

14.1. ....

14.2. ....

14.3. ....

14.4. ....

14.5. ....

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 SWZ – wzór Oświadczenia o braku podstaw wykluczenia**

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

**Oświadczenie o braku podstaw wykluczenia**

**DPIZP.2610.10.2021**

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami**” oświadczam (-y), że na dzień złożenia niniejszego oświadczenia aktualne pozostają informacje zawarte w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, tj. nie podlegam(-y) wykluczeniu na podstawie:

1. art. 108 ust. 1 pkt 3 ustawy,
2. art. 108 ust. 1 pkt 4 ustawy dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
3. art. 108 ust. 1 pkt 5 ustawy dotyczących zawarcia z innymi Wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
4. art. 108 ust. 1 pkt 6 ustawy,
5. art. 109 ust. 1 pkt 1 ustawy odnośnie do naruszenia obowiązków dotyczących płatności podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz.U. z 2019 r. poz. 1170 z późn. zm.),
6. art. 109 ust. 1 pkt 2 lit. b ustawy dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,
7. art. 109 ust. 1 pkt 2 lit. c ustawy,
8. art. 109 ust. 1 pkt 3 ustawy dotyczących ukarania za wykroczenie, za które wymierzono karę ograniczenia wolności lub karę grzywny,
9. art. 109 ust. 1 pkt 5-10 ustawy.

**Załącznik nr 3 do SWZ – wzór Oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej**

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

**Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej  
DPIZP.2610.10.2021**

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami” oświadczam(-y), że:

1. **nie należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j.: Dz. U. z 2021 r., poz. 275) z **żadnym z Wykonawców, którzy złożyli odrębną ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego<sup>1</sup>.
2. **należę(-ymy) do grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j.: Dz. U. z 2021 r., poz. 275) z **następującymi Wykonawcami, którzy złożyli odrębną ofertę w przedmiotowym postępowaniu** o udzielenie zamówienia publicznego<sup>1</sup>:

Lp.	Nazwa podmiotu	Siedziba
1		
(...)		

Jednocześnie na potwierdzenie, że nasza oferta została przygotowana niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej składam(-y) następujące informacje i/lub dokumenty:

.....  
 .....  
 .....  
 .....  
 .....  
 .....  
 .....  
 .....  
 .....  
 .....

**UWAGA:**

<sup>1</sup> niepotrzebne skreślić

**Załącznik nr 4 do SWZ – wzór Oświadczenia o podziale obowiązków w trakcie realizacji zamówienia**

**Oświadczenie o podziale obowiązków w trakcie realizacji zamówienia**  
(dotyczy Wykonawców wspólnie ubiegających się o udzielenie zamówienia)

**DPIZP.2610.10.2021**

Działając w imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia: .....<sup>1</sup>, przystępując do udziału w postępowaniu o zamówienie publiczne na „**Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami**” oświadczam(-y), że wyszczególnione poniżej dostawy/usługi zostaną zrealizowane zgodnie z poniższym:

1. Wykonawca .....<sup>2</sup> wykona następujące usługi/dostawy w ramach realizacji zamówienia:
  - 1.1. ....
  - 1.2. ....
  - 1.3. ....
2. Wykonawca .....<sup>2</sup> wykona następujące usługi/dostawy w ramach realizacji zamówienia:
  - 2.1. ....
  - 2.2. ....
  - 2.3. ....
3. Wykonawca .....<sup>2</sup> wykona następujące usługi/dostawy w ramach realizacji zamówienia:
  - 3.1. ....
  - 3.2. ....
  - 3.3. ....

**UWAGA:**

<sup>1</sup> należy wpisać firmy wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia

<sup>2</sup> należy wpisać firmy i adresy poszczególnych Wykonawców wspólnie ubiegających się o udzielenie zamówienia

**Załącznik nr 5 do SWZ – wzór Oświadczenia – Wykaz usług**  
*[warunek udziału w postępowaniu]*

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

**Oświadczenie – Wykaz usług**

**DPIZP.2610.10.2021.**

Przystępując do udziału w postępowaniu o zamówienie publiczne na „**Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami**”, składam(-y) wykaz usług 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 Rozdz. III.2. pkt 1.1.1. SWZ.

Lp.	Przedmiot wykonanych/wykonywanych usług (wg warunku udziału w postępowaniu)	Wartość brutto usługi w zł (w przypadku, gdy zakres usługi jest szerszy, należy podać wyłącznie wartość usługi odpowiadającej treści warunku udziału w postępowaniu w badanym zakresie, wg warunku udziału w postępowaniu)	Podmiot na rzecz którego wykonano usługę (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								
3								

**Uwaga do kol. 7:**

1. Do wykazu należy dołączyć dowody potwierdzające, że powyższe usługi zostały wykonane lub są wykonywane należycie, tj.:

- 1.1. referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane lub są wykonywane należycie, z tym, że w odniesieniu do nadal wykonywanych usług okresowych lub ciągłych referencje bądź inne dokumenty powinny być wydane nie wcześniej niż 3 m-cie przed upływem terminu składania ofert;
  - 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 zostały wykonane lub są wykonywane należycie (podać numer strony);

**Uwaga do kol. 8:**

1. Zaznaczyć „TAK”, tylko w przypadku, gdy Wykonawca polega na zdolnościach podmiotu udostępniającego zasoby dla wykazania spełnienia warunku udziału;
2. Dla wykazania spełniania warunku udziału w postępowaniu, opisanego w Rozdz. III.2. pkt 1.1.1.SWZ, Wykonawca może polegać na zdolnościach podmiotu udostępniającego zasoby, na zasadach określonych w art. 118 Ustawy. W tym celu Wykonawca składa podmiotowe środki dowodowe zgodnie z zasadami określonymi w Rozdz. IV.5. SWZ.

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

**Oświadczenie – Wykaz osób  
które będą uczestniczyć w wykonywaniu zamówienia  
DPIZP.2610.10.2021**

Przystępując do udziału w postępowaniu o zamówienie publiczne na „Rozbudowę platformy sprzętowej firewall (serwery appliance) wraz z oprogramowaniem i wsparciem na okres 36 miesięcy oraz usługą wdrożenia i konsultacjami”, składamy wykaz osób, które będą uczestniczyć w wykonaniu zamówienia na potwierdzenie spełnienia warunku udziału w postępowaniu, o którym mowa w Rozdziale III.2 pkt 1.1.2. SWZ:

**1. Jedną osobą spełniającą poniższe wymagania:**

Wymagania Zamawiającego wskazane w SWZ		Wypełnia Wykonawca	
Osoba, która posiada: 1) co najmniej 12 miesięczne doświadczenie przy realizacji zamówień o zakresie jak w pkt 1.1.1. z wyłączeniem wartości zamówień; 2) certyfikat PCNSE Palo Alto Networks Certified Network Security Engineer lub równoważny.	1.1	Imię i Nazwisko	
	1.2.	Wskazana osoba spełnia wymagania zdefiniowane w Rozdziale III.2 pkt 1.1.2.SWZ	
		Posiadane doświadczenie	1.2.1. Nazwa projektu 1.2.2. okres udziału w projekcie [DD-MM-RRRR – DD-MM-RRRR] 1.2.3. Podmiot na rzecz którego zrealizowano projekt
	1.3	Posiadany certyfikat	1.3.1. Nazwa certyfikatu 1.3.2. Podmiot wydający certyfikat
<b>UWAGA 2</b>			

<p>Przez certyfikat równoważny, o którym mowa powyżej Zamawiający rozumie certyfikat, który:</p> <ol style="list-style-type: none"> <li>1) jest analogiczny co do zakresu z przykładowym certyfikatem wskazanym z nazwy dla danej roli, co jest rozumiane jako:             <ol style="list-style-type: none"> <li>a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,</li> <li>b) analogiczny stopień poziomu kompetencji,</li> <li>c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu,</li> </ol> </li> <li>2. potwierdzony jest egzaminem (dotyczy tylko tych ról, których przykładowe certyfikaty muszą być potwierdzone egzaminem).</li> </ol> <p><u>Uwaga:</u></p> <ol style="list-style-type: none"> <li>1. Dla wykazania spełnienia warunku udziału w postępowaniu opisanego w rozdziale III.2 pkt 1.1.2. SWZ, Wykonawca może polegać, na zasadach określonych w art. 118 ustawy, na osobach zdolnych do wykonania zamówienia oddanych mu do dyspozycji przez inne podmioty.</li> <li>2. W odniesieniu do podstawy dysponowania osobą Wykonawca wypełnia kolumnę „Dysponowanie bezpośrednie” albo „Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych”.</li> <li>3. W przypadku dysponowania przez Wykonawcę osobą na podstawie art. 118 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 SWZ</li> </ol>				<p>1.3.3</p> <p>1.3.4</p> <p>1.4.1</p> <p>1.4.2</p>	<p>Nr certyfikatu [o ile dotyczy]</p> <p>Data ważności certyfikatu [DD-MM-RRRR] [o ile dotyczy]</p> <p>Dysponowanie bezpośrednie</p> <p>Dysponowanie osobą na podstawie art. 118 ustawy – Prawo zamówień publicznych</p>
--	--	--	--	---	--

**Załącznik nr 7 do SWZ – projektowane postanowienia umowy**

**Projektowane postanowienia umowy**

Umowa nr \_\_\_\_\_/DI/2021/2610

zawarta w dniu \_\_\_\_\_ 2021 r. w Warszawie pomiędzy:

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

\_\_\_\_\_ – Zastępca Prezesa ARiMR, pełnomocnik;  
\_\_\_\_\_ – Dyrektor Departamentu Księgowości, w ramach zajmowanego stanowiska wykonująca obowiązki Głównego Księgowego, pełnomocnik;

a

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_, zwaną dalej **„Wykonawcą”**, którą reprezentuje:

\_\_\_\_\_ – \_\_\_\_\_;

zwanych łącznie **„Stronami”**,

w wyniku wyboru oferty w postępowaniu o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego zgodnie z art. 132-139 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 t.j. z późn. 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 wielkiej litery w celu podkreślenia, że jest to pojęcie zdefiniowane:

- 1) **Strony** – Zamawiający i Wykonawca;
- 2) **Umowa** – niniejsza umowa wraz z załącznikami określająca prawa i obowiązki Stron z niej wynikające i związane z jej wykonaniem;
- 3) **Sprzęt IT** – urządzenia informatyczne, pełniące funkcje zapory sieciowej wraz z systemem zarządzania oraz Oprogramowaniem niezbędnym do zachowania wyspecyfikowanej funkcjonalności Sprzętu IT, szczegółowo opisane w Załączniku nr 1 oraz Załączniku nr 7;
- 4) **Oprogramowanie** – programy komputerowe dostarczone przez Wykonawcę, z których Zamawiający korzysta na podstawie Licencji udzielonych przez producenta, niezbędne do korzystania ze Sprzętu IT;
- 5) **Licencja** – prawo do terminowego (3 letniego) 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 Wykonawcę, mające na celu uruchomienie dostarczonego Sprzętu IT, instalacje Oprogramowania oraz przeniesienie funkcjonalności z dotychczas użytkowanych urządzeń firewall pracujących w strefie DMZ na Sprzęt IT – szczegółowo opisane w Załączniku nr 1;
- 8) **Projekt techniczny** – dokumentacja projektowa, wykonana przez Wykonawcę i odebrana przez Zamawiającego, szczegółowo określająca i opisująca wszelkie elementy sieci LAN u Zamawiającego, zakres i opis wykonywanych prac, kontrolę jakości prac i odbiory prac, instalacje i wyposażenie techniczne, zastosowane technologie, rozwiązania techniczne, specyfikacje produktowe, procedury konfiguracyjne oraz procedury testowe dla tworzonej sieci LAN u



Zamawiającego wraz z rysunkami i schematami połączeń elektrycznych i logicznych Sprzętu IT - szczegółowo opisany w Załączniku nr 1 do Umowy

- 9) **Dokumentacja powykonawcza** – dokumentacja zawierająca schemat fizyczny i logiczny podłączenia Sprzętu IT, konfigurację Sprzętu IT oraz zapis zastosowanych rozwiązań i technologii;
- 10) **Dokumenty** – instrukcje eksploatacyjne, instrukcje obsługi Sprzętu IT oraz dokumenty licencyjne dla Oprogramowania;
- 11) **COPD** – Centralne Ośrodki Przetwarzania Danych Zamawiającego znajdujące się w Piasecznie, ul. Jana Pawła II 66, 05-500 Piaseczno oraz w Warszawie, ul. Poleczki 33, 02-822 Warszawa;
- 12) **Dni Robocze** – okres w godzinach 7.30-15.30 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych od pracy u Zamawiającego, o których Zamawiający powiadomi Wykonawcę.

## § 2.

### Przedmiot Umowy

1. Na podstawie Umowy Wykonawca:
  - 1) sprzedaje i dostarcza Zamawiającemu fabrycznie nowy Sprzęt IT zgodnie ze Specyfikacją techniczną Sprzętu IT stanowiącą Załącznik nr 1 do Umowy oraz Formularzem ofertowym Wykonawcy stanowiącym Załącznik nr 7 Umowy;
  - 2) wykona Projekt techniczny;
  - 3) przeprowadzi Wdrożenie zgodnie z zasadami określonymi w § 4 ust. 6-7 Umowy oraz w załączniku nr 1 do Umowy;
  - 4) dostarczy Dokumenty i Dokumentację powykonawczą;
  - 5) będzie świadczył Serwis gwarancyjny dla Sprzętu IT oraz Oprogramowania przez okres 36 miesięcy.
2. Wraz z dostawą Sprzętu IT oraz Oprogramowania Wykonawca dostarczy Zamawiającemu Dokumenty.
3. W ramach Umowy Wykonawca wykona Dokumentację powykonawczą i dostarczy ją Zamawiającemu w formie elektronicznej do akceptacji i odbioru.
4. W ramach Umowy Wykonawca zapewni Zamawiającemu 300 godzin konsultacji technicznych w okresie trwania Serwisu gwarancyjnego, jednak nie mniej niż 150 godzin. Konsultacje będą obejmowały analizy, audyty oraz rekomendacje dotyczące Sprzętu IT lub Oprogramowania, jak również wszelkiego rodzaju prace konfiguracyjne Sprzętu IT lub Oprogramowania oraz pomoc przy pracach technicznych przeprowadzonych przez Zamawiającego w COPD. Konsultacje będą świadczone w języku polskim. Zamawiający zastrzega sobie prawo niewykorzystania pełnej ilości godzin konsultacji powyżej zastrzeżonego minimum. Wykonawcy z tytułu niewykorzystania pełnej ilości konsultacji nie przysługują żadne roszczenia odszkodowawcze.
5. W ramach konsultacji technicznych Wykonawca na wniosek Zamawiającego przeprowadzi warsztaty lub prezentacje dotyczące wskazanego elementu Sprzętu IT lub Oprogramowania w Centrali Zamawiającego przy ul. Poleczki 33 w Warszawie. Czas dojazdu do Zamawiającego nie będzie wliczony jako wykorzystanie dostępnej puli godzin. Zamawiający dopuszcza przeprowadzenie konsultacji w formie zdalnej. Decyzję o formie przeprowadzenia konsultacji każdorazowo podejmie Zamawiający.
6. Wykonawca będzie przyjmował zgłoszenia konsultacyjne od poniedziałku do piątku, w godz. 9-15, telefonicznie pod numerem tel. .... lub na adres poczty elektronicznej ..... Przyjęcie zgłoszenia zostanie potwierdzone przez Wykonawcę drogą elektroniczną na adresy e-mail osób wskazanych przez Zamawiającego w Umowie w ciągu 1 godziny od otrzymania zgłoszenia. O każdej zmianie adresu e-mail lub numeru telefonu wskazanego powyżej Wykonawca zobowiązany jest niezwłocznie powiadomić Zamawiającego za pośrednictwem poczty elektronicznej.
7. Na koniec każdego kwartału Wykonawca przedstawi Raport kwartalny zawierający informacje o zgłoszonych i przeprowadzonych konsultacjach, którego wzór został określony w Załączniku nr 4b do Umowy.

## § 3.

### Wymagania dotyczące wykonania Umowy

1. Wykonawca oświadcza, że:
  - 1) jest upoważniony do sprzedaży Sprzętu IT oraz do przekazania Licencji, uprawniającej do korzystania przez Zamawiającego z Oprogramowania;
  - 2) posiada konieczne doświadczenie i profesjonalne kwalifikacje niezbędne do prawidłowego wykonania Umowy i zobowiązuje się do wykonania Umowy przy zachowaniu najwyższej staranności określonej w art. 355 § 2 Kodeksu cywilnego.
2. W ramach Umowy Wykonawca zapewni Zamawiającemu prawo do korzystania z Oprogramowania na warunkach niezbędnych do korzystania ze Sprzętu IT oraz dostarczy stosowne dokumenty licencyjne wystawione przez producenta Sprzętu.

3. Osobami upoważnionymi do uzgadniania na bieżąco spraw związanych z realizacją Umowy i podpisywania raportów i protokołów odbioru, przy czym związanymi warunkami, w tym terminami określonymi w Umowie są:

po stronie Zamawiającego:

\_\_\_\_\_, tel. \_\_\_\_\_; e-mail: \_\_\_\_\_@arimr.gov.pl

\_\_\_\_\_, tel. \_\_\_\_\_; e-mail: \_\_\_\_\_@arimr.gov.pl

\_\_\_\_\_, tel. \_\_\_\_\_; e-mail: \_\_\_\_\_@arimr.gov.pl

po stronie Wykonawcy:

\_\_\_\_\_, tel. \_\_\_\_\_; e-mail: \_\_\_\_\_@\_\_\_\_\_

\_\_\_\_\_, tel. \_\_\_\_\_; e-mail: \_\_\_\_\_@\_\_\_\_\_

przy czym zmiana ww. osób i danych nie wymaga zawierania pisemnego aneksu do Umowy, a jedynie pisemnego poinformowania drugiej Strony o zmianie.

4. Wykonawca oświadcza, że dostarczony Sprzęt oraz Oprogramowanie są wolne od oprogramowania szkodliwego i szpiegującego, a także są zabezpieczone przed nieautoryzowanym dostępem.
5. Wykonawca 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.
6. Zamawiający wymaga, a Wykonawca oświadcza, że Wdrożenie będzie wykonywane bezpośrednio przez minimum 1 osobę posiadającą uprawnienia PCNSE Palo Alto Networks Certified Network Security Engineer lub równoważne. pracujących w strefie DMZ 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. Nowa osoba musi posiadać kwalifikacje i doświadczenie nie gorsze od osoby wskazanej w Wykazie osób złożonym wraz z ofertą. Zmiana osoby, o której mowa w zdaniu poprzedzającym nie wymaga formy aneksu.
7. W terminie do 3 Dni Roboczych po podpisaniu przez upoważnionych przedstawicieli Stron Umowy, Zamawiający przekaże Wykonawcy aktualną konfigurację urządzeń, o których mowa w ust. 5 oraz zapisy konfiguracji do przeniesienia z urządzeń firewall pracujących w strefie DMZ pracujących w sieci LAN Zamawiającego.

#### § 4.

##### Termin realizacji Umowy

1. Dostarczenie Sprzętu IT oraz Oprogramowania, Dokumentów oraz Wdrożenie nastąpi w COPD nie później niż w terminie do [.....] Dni Roboczych od dnia zawarcia Umowy. *(Maksymalny termin wynosi 45 Dni Roboczych, zapis zostanie uzupełniony zgodnie z Formularzem Ofertowym Wykonawcy).*
2. Wykonawca powiadomi 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. Dostarczenie Sprzętu IT wraz z Oprogramowaniem i Dokumentów odbędzie się na koszt i ryzyko Wykonawcy. Wykonawca dostarczy Sprzęt IT wraz z Oprogramowaniem i Dokumenty zgodnie z warunkami Umowy i poniesie pełne ryzyko związane z niebezpieczeństwem utraty albo uszkodzenia Sprzętu.
4. Odbiór Sprzętu IT wraz z Oprogramowaniem oraz Dokumentów zostanie dokonany komisyjnie z udziałem upoważnionych przedstawicieli Stron. Odbiór i zawiadomienia o terminach odbiorów i Wdrożenia będą dokonywane w Dniach Roboczych.
5. Podczas odbioru Sprzętu IT wraz z Oprogramowaniem oraz Dokumentów Wykonawca w obecności Zamawiającego:
- 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 Załącznikiem nr 7;
  - 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 oraz Załącznikiem nr 1
6. W ramach Wdrożenia Wykonawca w obecności pracownika Zamawiającego:
- 1) przygotuje konfigurację dostarczonego Sprzętu IT (konfiguracja podstawowa – adresacja IP, konfiguracja klastra rozciągniętego na dwie lokalizacje);
  - 2) przeniesie listy kontroli dostępu z urządzeń firewall pracujących w strefie DMZ i z przełączników Zamawiającego 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 dostarczanego Sprzętu IT, utworzenie i konfiguracja kont użytkowników);
  - 4) uruchomi Sprzęt IT produkcyjnie z pełnymi funkcjonalnościami.
7. Po dokonaniu przez Zamawiającego bez zastrzeżeń odbioru Sprzętu IT wraz z Oprogramowaniem i Dokumentami oraz wykonaniu Wdrożenia w ostatniej lokalizacji COPD, Zamawiający podpisze Protokół odbioru, którego wzór stanowi Załącznik nr 3 do Umowy.

8. W przypadku stwierdzenia podczas odbioru, że:
  - 1) Sprzęt IT lub Oprogramowania są niezgodne z Załącznikiem nr 1 lub Załącznikiem nr 7 lub posiadają ślady zewnętrznego uszkodzenia lub
  - 2) nie dostarczono wszystkich wymaganych Dokumentów;
  - 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, Zamawiający odmówi podpisania Protokołu odbioru, jednocześnie przekaże Wykonawcy protokół przedstawiający powód odmowy odbioru ze wskazaniem terminu dostarczenia Sprzętu IT wraz z Oprogramowaniem lub Dokumentów lub wolnych od wad lub ponownego wykonania Wdrożenia. Procedura czynności odbioru zostanie przeprowadzona ponownie.
9. W przypadku stwierdzenia podczas powtórnej procedury odbioru którejkolwiek z okoliczności wskazanych w ust. 8 Zamawiający odmówi odbioru przedmiotu Umowy i jednocześnie przekaże Wykonawcy protokół przedstawiający powód odmowy odbioru Sprzętu IT wraz z Oprogramowaniem, Dokumentów lub wykonania Wdrożenia. W przypadku odmowy ponownego odbioru któregośkolwiek z elementów przedmiotu Umowy Wykonawca ma obowiązek odbioru dostarczonego Sprzętu lub Dokumentów z miejsca dostarczenia w terminie 5 Dni Roboczych od dnia przekazania Wykonawcy protokołu przedstawiającego powody odmowy odbioru Sprzętu IT.
10. W terminie do:
  - 1) 10 Dni Roboczych od dnia podpisania Umowy, Wykonawca dostarczy Zamawiającemu Projekt techniczny. Odbiór zostanie potwierdzony Protokołem odbioru Projektu technicznego, którego wzór stanowi Załącznik nr 3. Zamawiający zastrzega sobie prawo zgłaszania uwag do Projektu technicznego. Wykonawca zobowiązany jest uwzględnić uwagi Zamawiającego lub zgłosić zastrzeżenia w terminie 3 Dni Roboczych od dnia otrzymania uwag Zamawiającego;
  - 2) 8 Dni Roboczych od dnia podpisania Protokołu odbioru, o którym mowa w ust. 7, Wykonawca dostarczy Zamawiającemu Dokumentację powykonawczą. Odbiór zostanie potwierdzony Protokołem odbioru Dokumentacji powykonawczej, którego wzór stanowi Załącznik nr 3 4. Zamawiający zastrzega sobie prawo zgłaszania uwag do Dokumentacji powykonawczej. Wykonawca zobowiązany jest uwzględnić uwagi Zamawiającego lub zgłosić zastrzeżenia w terminie 3 Dni Roboczych od dnia otrzymania uwag Zamawiającego.
11. Wszystkie powiadomienia dotyczące odbiorów Sprzętu IT wraz z Oprogramowaniem, Dokumentów, Projektu technicznego, Dokumentacji powykonawczej lub wykonania Wdrożenia powinny być dokonywane w Dni Robocze.

#### **§ 5.**

##### **Udzielenie licencji**

1. Zamawiający, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2 Umowy, nabywa Licencje do Oprogramowania wskazane w załączniku nr 1, upoważniającą do korzystania z Oprogramowania przez okres 3 lat w celu zachowania funkcjonalności Sprzętu IT.
2. Zamawiający, 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 jakiegokolwiek formie w zakresie, w którym jest to niezbędne dla wprowadzenia, wyświetlania, stosowania, przekazywania, przechowywania Oprogramowania dla własnych potrzeb Zamawiającego, z uwzględnieniem treści ust. 3, zgodnie z jego charakterem i przeznaczeniem, Dokumentami i warunkami Umowy.
3. Licencja uzyskana zgodnie z treścią ust. 2 może być wykorzystywana wyłącznie dla celów działalności Zamawiającego i nie obejmuje prawa do wprowadzenia 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 Zamawiający 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 Wykonawcę przez okres 36 miesięcy od dnia podpisania Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w §4 ust. 10 Umowy.
2. Wykonawca zobowiązuje się, że podczas trwania Serwisu gwarancyjnego, po otrzymaniu zgłoszenia serwisowego od Zamawiającego, 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 Wykonawcę 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 Wykonawca 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. Wykonawca, 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 Wykonawcę czwartego zgłoszenia serwisowego dotyczącego tego samego Sprzętu IT. W przypadku, gdy dostarczenie takiego samego Sprzętu IT nie będzie możliwe, Wykonawca dostarczy nowy sprzęt o parametrach technicznych nie gorszych od określonych w Załączniku nr 1 i 7 do Umowy. Dostarczenie zastępcze wymaga zgody Zamawiającego.
6. Wykonawca będzie przyjmował zgłoszenia serwisowe Zamawiającego od osób wskazanych przez Zamawiającego w trybie 24 godziny na dobę 7 dni w tygodniu (tryb 24/7) telefonicznie pod numerem ....., lub na adres poczty elektronicznej ..... Przyjęcie zgłoszenia zostanie przez Wykonawcę potwierdzone (drogą elektroniczną na wskazany przez Zamawiającego adres e-mail) w ciągu 1 godziny od otrzymania zgłoszenia. Niepotwierdzenie zgłoszenia w powyższym terminie Zamawiający uznaje za przyjęcie zgłoszenia. O każdej zmianie adresu lub numerów telefonów wskazanych powyżej, Wykonawca zobowiązany jest niezwłocznie powiadomić na piśmie Zamawiającego. 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 nr 7 do Umowy.
8. Wszelkie koszty związane ze świadczeniem Serwisu gwarancyjnego obciążają Wykonawcę.
9. Niezależnie od uprawnień z tytułu Serwisu gwarancyjnego (gwarancji) Zamawiającemu przysługują wobec Wykonawcy uprawnienia z tytułu rękojmi. Jeżeli w ramach rękojmi Zamawiający zażąda wykonania przez Wykonawcę 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. Zamawiający zastrzega sobie prawo do zmiany lokalizacji COPD. Zamawiający odinstaluje, przewiezie, dokona instalacji i uruchomi Sprzęt IT w nowej lokalizacji COPD. Uruchomienie Sprzętu IT odbędzie się w asyście przedstawiciela Wykonawcy, jeśli Wykonawca poinformuje Zamawiającego o zamiarze uczestniczenia w uruchomieniu Sprzętu IT w nowej lokalizacji COPD. Nieobecność przedstawiciela Wykonawcy podczas uruchomienia Sprzętu IT w nowej lokalizacji nie wpływa na uruchomienie przez Zamawiającego Sprzętu IT oraz nie zwalnia Wykonawcy 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 Wykonawcę w § 3 ust. 3 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, Wykonawca świadczycy będzie zobowiązania wynikające z Umowy dla zmienionej lokalizacji COPD.
11. W ramach Serwisu gwarancyjnego Zamawiający będzie miał prawo dostępu do serwisu producenta Oprogramowania, w tym do:
  - 1) aktualizacji wersji Oprogramowania (*updates, upgrade, patches*) oraz nowych wersji Oprogramowania i udoskonalień do wersji bieżących Oprogramowania (nowych edycji Oprogramowania, wydań uzupełniających, poprawek programistycznych); Zamawiający, w ramach wynagrodzenia, uzyskuje prawo do zainstalowania uruchomienia, przechowywania i nieograniczonego w czasie korzystania z aktualizacji;
  - 2) monitorowania statusu zgłoszeń serwisowych;
  - 3) samodzielnego oraz za pośrednictwem Wykonawcy zgłaszania awarii do producenta;
  - 4) samodzielnego oraz za pośrednictwem Wykonawcy 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.
12. W przypadku naprawy poza siedzibą Agencji lub wymiany gwarancyjnej nośników pamięci nieulotnej w każdym przypadku uszkodzone nośniki lub nośniki z uszkodzonych modułów, pozostają u Zamawiającego.
13. Po 12 miesiącach świadczenia Serwisu gwarancyjnego Wykonawca przedłoży Zamawiającemu do akceptacji raport z realizacji Serwisu gwarancyjnego.

## § 7.

### Wynagrodzenie

1. łączne wynagrodzenie z tytułu wykonania Umowy wynosi netto .....(słownie złotych:.....), powiększone o należny VAT, co daje kwotę brutto ..... (słownie złotych:.....), z czego:

- 1) wynagrodzenie za sprzedaż i dostarczenie Sprzętu IT wraz z Oprogramowaniem oraz Projektu technicznego, Wdrożenie i Dokumentację powykonawczą wynosi netto .....(słownie złotych:.....), powiększone o należny podatek od towarów i usług (VAT), co daje kwotę brutto ..... (słownie złotych:.....),
  - 2) wynagrodzenie za Serwis gwarancyjny wynosi netto .....(słownie złotych:.....), powiększone o należny VAT, co daje kwotę brutto ..... (słownie złotych:.....),
  - 3) maksymalne wynagrodzenie z tytułu konsultacji, o których mowa w § 2 ust. 4 Umowy wynosi netto .....(słownie złotych:.....), powiększone o należny VAT, co daje kwotę brutto ..... (słownie złotych:.....).
2. Wynagrodzenie, o którym mowa :
    - 1) w ust. 1 pkt 1 będzie płatne na podstawie faktury VAT wystawionej przez Wykonawcę, w terminie do 28 dni licząc od daty otrzymania przez Zamawiającego 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 do wystawienia faktury VAT;
    - 2) w ust. 1 pkt 2 będzie płatne w 3 równych częściach na podstawie faktury VAT wystawionej przez Wykonawcę, przy czym dla 1 części - w terminie do 28 dni licząc od daty otrzymania przez Zamawiającego 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. Wykonawca będzie uprawniony do wystawienia faktur VAT za część 2 i 3 wynagrodzenia odpowiednio po upływie 12 i 24 miesięcy od dnia zawarcia Umowy, przy czym nie później niż 2 grudnia 2022 r. (za cz. 2) i 2 grudnia 2023 r. (za cz. 3) Wynagrodzenie, o którym mowa w zdaniu poprzednim będzie płatne w terminie do 28 dni licząc od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT łącznie z zaakceptowanym przez Zamawiającego Raportem z Serwisu gwarancyjnego, o którym mowa w § 6 ust. 12 Umowy;
    - 3) ust. 1 pkt 3 będzie płatne na podstawie faktury VAT wystawionej przez Wykonawcę, w terminie do 28 dni licząc od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT łącznie z podpisanym bez zastrzeżeń przez upoważnionych przedstawicieli Stron Raportem z przeprowadzonych konsultacji, o którym mowa w § 2 ust. 7 Umowy. Wynagrodzenie za konsultacje rozliczane jest kwartalnie i wyliczane jako iloczyn ilości godzin konsultacji odebranych w danym kwartale i ceny za jedną roboczogodzinę konsultacji określoną zgodnie z ofertą Wykonawcy na kwotę netto ..... powiększoną o należny podatek VAT, przy czym ostatecznie rozliczenie kwartalne uwzględniać będzie minimalną ilość za konsultacje, o których mowa w § 2 ust. 4 Umowy.
  3. Wynagrodzenie, o którym mowa w ust. 1 wyczerpuje wszelkie roszczenia finansowe Wykonawcy z tytułu wykonania Umowy, w tym uwzględnia konsultacje, o których mowa w § 2 ust. 4 Umowy.
  4. Błędnie wystawiona faktura VAT lub brak podpisanego przez Strony Protokołu odbioru Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 Umowy lub brak raportu, o którym mowa w § 6 ust. 12, spowodują naliczenie ponownego 28-dniowego terminu płatności od momentu dostarczenia poprawionych lub brakujących dokumentów.
  5. Za termin wykonania płatności uznaje się dzień obciążenia rachunku bankowego Zamawiającego.
  6. W przypadku niezgodności, w dniu realizacji płatności numeru rachunku bankowego wskazanego przez Wykonawcę na fakturze z numerem rachunku bankowego zamieszczonym w wykazie podmiotów, o których mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2021 r., poz. 685 z późn. zm.), Strony ustalają, że realizacja płatności nastąpi w trybie art. 108a ww. ustawy.
  7. Jeżeli w trakcie realizacji Umowy nastąpi:
    - 1) zmiana stawki podatku od towarów i usług lub podatku akcyzowego,
    - 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,
    - 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 (Dz. U. poz. 2215 oraz z 2019r. poz. 1074 i 1572), a zmiany te będą miały wpływ na koszty wykonania Umowy – zastosowanie mają zasady wprowadzania zmian wysokości wynagrodzenia należnego Wykonawcy określone w ust. 8 poniżej.
  8. Zmiana wysokości wynagrodzenia wymaga zmiany Umowy w drodze aneksu.
  9. Wykonawca najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 7 uprawniony jest do wystąpienia do Zamawiającego z pisemnym wnioskiem o dokonanie zmiany Umowy w zakresie wysokości wynagrodzenia wraz z jej uzasadnieniem oraz dokumentami niezbędnymi do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 7, mają wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia Wykonawcy określonego w niniejszej Umowie, a w szczególności:
    - 1) szczegółową kalkulację proponowanej zmienionej wysokości wynagrodzenia Wykonawcy oraz wykazanie adekwatności propozycji do zmiany wysokości kosztów wykonania Umowy przez Wykonawcę.

- 2) przyjęte przez Wykonawcę 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, Zamawiający może zwrócić się do Wykonawcy o jego uzupełnienie lub przekazanie dodatkowych wyjaśnień lub dokumentów (np. zażądać: oryginałów do wglądu, przekazania kopii dokumentów potwierdzonych za zgodność z oryginałami).
  11. Zamawiający 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 Wykonawcy.
  12. Zamawiający najpóźniej w terminie 30 dni od dnia wejścia w życie przepisów wprowadzających zmiany, o których mowa w ust. 7 może przekazać Wykonawcy 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, Zamawiający może zwrócić się do Wykonawcy o złożenie wyjaśnień lub dokumentów (oryginałów do wglądu lub kopii potwierdzonych za zgodność z oryginałem) niezbędnych do oceny przez Zamawiającego, czy zmiany, o których mowa w ust. 7, mają wpływ na koszty wykonania Umowy przez Wykonawcę oraz w jakim stopniu zmiany tych kosztów uzasadniają zmianę wysokości wynagrodzenia. Rodzaj i zakres tych informacji określi Zamawiający. Postanowienia ust. 10-15 stosuje się odpowiednio, z tym, że Wykonawca jest zobowiązany w każdym przypadku do zajęcia pisemnego stanowiska w terminie 30 dni od dnia otrzymania wniosku od Zamawiającego.
  14. W przypadku niewykonania lub nienależytego wykonania przez Wykonawcę zobowiązania określonego w ust. 13 w terminie określonym w ust. 13, Wykonawca zapłaci na rzecz Zamawiającego karę umowną w wysokości 0,2 % łącznego wynagrodzenia brutto określonego w § 7 ust.1 za każdy rozpoczęty dzień zwłoki. Jeżeli w terminie określonym w ust. 13 Wykonawca nie przedłoży wyjaśnień lub dokumentów, o których mowa w ust. 9 lub przedłożone przez Wykonawcę wyjaśnienia lub dokumenty będą niewystarczające do dokonania przez Zamawiającego oceny, o której mowa w ust. 13 – Zamawiający wyznaczy Wykonawcy dodatkowy termin, nie dłuższy niż 10 dni, na dostarczenie lub uzupełnienie wyjaśnień lub dokumentów. W przypadku bezskutecznego upływu terminu wyznaczonego zgodnie ze zdaniem drugim, Wykonawca 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.
  16. Zasady zmiany wynagrodzenia określone w ust. 7 – 15 powyżej mają odpowiednie zastosowanie do zmiany wysokości wynagrodzenia w przypadku zmiany średniorocznego wskaźnika cen towarów i usług konsumpcyjnych ogółem ogłaszanego w komunikacie Prezesa Głównego Urzędu Statystycznego na podstawie przepisów ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (dalej „wskaźnik”), z zastrzeżeniem następujących zasad:
    - 1) zmiana wynagrodzenia jest możliwa, gdy wskaźnik w stosunku do roku poprzedniego będzie wyższy niż 101,5 albo będzie niższy niż 98,5 (tj. wzrost poziomu cen o 1,5% albo spadek poziomu cen o 1,5%),
    - 2) zmiana wynagrodzenia obowiązuje w stosunku do wynagrodzenia, które stanie się należne dopiero po dniu podpisania aneksu do Umowy (w formie pisemnej pod rygorem nieważności), tym samym zmiana nie dotyczy wynagrodzenia ustalonego (wystawienie faktury) lub rozliczonego przed dokonaniem zmiany Umowy,
    - 3) zmiana wynagrodzenia możliwa jest najwcześniej po upływie 12 miesięcy od zawarcia Umowy), chyba że data zawarcia Umowy przypada 180 dni od daty złożenia oferty przez Wykonawcę, wówczas (i) zmiana wynagrodzenia możliwa jest po upływie 12 miesięcy od dnia otwarcia oferty Wykonawcy, (ii) a wartość zmiany wskaźnika zostanie ustalona nie względem roku poprzedniego, a względem roku, w którym doszło do otwarcia oferty Wykonawcy,
    - 4) z zastrzeżeniem limitu ustalonego w pkt 5, w przypadku zmiany wskaźnika, każdorazowa wartość zmiany wynagrodzenia za 1 rodzinę konsultacji będzie ustalana w następujący sposób:
      - a) jeśli zmiana wskaźnika będzie na poziomie powyżej 101,5 do 103 (wzrost poziomu cen od 1,5% do 3%) – wynagrodzenie za 1 godzinę konsultacji lub wynagrodzenie roczne za świadczenie Serwisu gwarancyjnego wzrośnie o 1% względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 98,5 do 97 (spadek poziomu cen od 1,5% do 3%) - wynagrodzenie za 1 godzinę konsultacji lub wynagrodzenie roczne za świadczenie Serwisu gwarancyjnego zmaleje o 1% względem wynagrodzenia, które w chwili zmiany wynika z Umowy,
      - b) jeśli zmiana wskaźnika będzie na poziomie powyżej 103 do 105 (wzrost poziomu cen od 3 % do 5 %) – wynagrodzenie za 1 godzinę konsultacji lub wynagrodzenie roczne za świadczenie Serwisu gwarancyjnego wzrośnie o 2 % względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 97 do 95 (spadek poziomu cen od 3% do 5%) - wynagrodzenie za 1 godzinę konsultacji miesięczne lub wynagrodzenie roczne za świadczenie Serwisu gwarancyjnego zmaleje o 2% względem wynagrodzenia, które w chwili zmiany wynika z Umowy,

- c) jeśli zmiana wskaźnika będzie na poziomie powyżej 105 (wzrost poziomu cen ponad 5%) - wynagrodzenie za 1 godzinę konsultacji lub wynagrodzenie roczne za świadczenie Serwisu gwarancyjnego zmieni się o 3,5% względem wynagrodzenia, które w chwili zmiany wynika z Umowy, a jeśli zmiana wskaźnika będzie na poziomie poniżej 5 (spadek poziomu cen o ponad 5%) - wynagrodzenie za 1 godzinę konsultacji miesięczne lub wynagrodzenie roczne za świadczenie Serwisu gwarancyjnego zmaleje o 3,5% względem wynagrodzenia, które w chwili zmiany wynika z Umowy;
  - 5) W okresie obowiązywania Umowy zmiana wskaźnika skutkować może zmianą wynagrodzenia Wykonawcy nie więcej niż o 10 % w stosunku do wartości wskazanej w ofercie;
  - 6) zmiany wynagrodzenia zgodnie z zasadami określonymi w niniejszym ustępie są możliwe do wysokości nieprzekraczającej łącznie 5% wartości wynagrodzenia określonego w § 7 ust. 1 Umowy;
  - 7) uprawnienie do wnioskowania o waloryzację wynagrodzenia zastrzeżone jest dla obu Stron Umowy.
17. Wykonawca, którego wynagrodzenie zostało zmienione w związku ze zmianą wskaźnika, o którym mowa w ust. 16, zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy. Wykonawca złoży oświadczenie w formie pisemnej, w którym potwierdzi fakt, iż dokonał zmiany wynagrodzenia należnego podwykonawcy oraz wskaże jego kwotę oraz datę zapłaty na rzecz podwykonawcy zmienionego wynagrodzenia. Przedmiotowe oświadczenie stanowić będzie załącznik do faktur wystawianych Zamawiającemu z tytułu zmienionego wynagrodzenia za realizację zobowiązań w ramach Umowy.

## § 8 .

### Kary umowne i roszczenia odszkodowawcze

1. W przypadku zwłoki Wykonawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem, Dokumentów oraz w realizacji Wdrożenia w terminie wskazanym w §4 ust. 1 lub ust. 2 Umowy Zamawiającemu przysługuje kara umowna w wysokości 4000,00 za każdy rozpoczęty dzień kalendarzowy zwłoki.
2. Jeśli zwłoka, o której mowa w ust. 1 będzie trwała dłużej niż 14 dni, Zamawiający 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% łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy.
3. W przypadku zwłoki w wymianie Sprzętu IT na fabrycznie nowy, wolny od wad w okresie Serwisu gwarancyjnego (gwarancji) lub rękojmi, w stosunku do terminów o których mowa w § 6 ust. 4 lub 5 Umowy, Zamawiającemu przysługuje kara umowna w wysokości 0,2 % 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 zwłoki, jeżeli termin jest liczony w godzinach.
4. Jeżeli zwłoka, a której mowa w ust. 3 będzie trwała dłużej niż 24 godziny (dla terminów liczonych w godzinach) lub odpowiednio 3 dni (dla terminów liczonych w dniach), Zamawiający, w terminie 14 dni od upływu terminu powyższego opóźnienia, ma prawo, według własnego wyboru:
  - 1) odstąpić od Umowy bez konieczności wyznaczenia dodatkowego terminu na usunięcie wad oraz zażądać kary umownej w wysokości 20 % kwoty łącznego wynagrodzenia brutto określonego w § 7 ust. 1 Umowy;
  - 2) dokonać zastępczej wymiany Sprzętu IT na koszt Wykonawcy;
  - 3) naliczyć 2-krotność kary umownej określonej w ust. 3, począwszy od odpowiednio 25 godziny zwłoki lub od 4 dnia zwłoki w stosunku do terminu, w którym zostanie wymieniony Sprzęt IT.
5. W razie zwłoki Wykonawcy w dostarczeniu Sprzętu IT wraz z Oprogramowaniem lub Dokumentów wolnych od wad lub ponownego wykonania Wdrożenia, w stosunku do terminu, określonego zgodnie z § 4 ust. 8, Wykonawca zapłaci karę umowną w wysokości 4000,00 za każdy rozpoczęty Dzień Roboczy zwłoki.
6. W razie zwłoki Wykonawcy w odbiorze Sprzętu IT wraz z Oprogramowaniem lub Dokumentów z miejsca dostarczenia w stosunku do terminu, o którym mowa w § 4 ust. 9, Wykonawca zapłaci karę umowną w wysokości 1000,00 zł za każdy rozpoczęty Dzień Roboczy zwłoki. W przypadku ponownej odmowy odbioru Sprzętu IT , o której mowa w § 4 ust. 9 Umowy, Zamawiający ma prawo odstąpić od Umowy w terminie 30 dni od daty przekazania Wykonawcy 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 od dnia odstąpienia.
7. W razie zwłoki Wykonawcy w dostarczeniu Dokumentacji powykonawczej w stosunku do terminu, o którym mowa w § 4 ust. 10, Wykonawca zapłaci karę umowną w wysokości 1000,00 za każdy rozpoczęty Dzień Roboczy zwłoki.
8. Jeżeli na skutek niewykonania lub nienależytego wykonania Umowy powstanie szkoda przewyższająca zastrzeżoną karę umowną, Zamawiającemu oprócz tej kary przysługuje prawo do dochodzenia odszkodowania uzupełniającego. Jeżeli

- szkoda powstanie z przyczyn innych niż te, ze względu, na które zastrzeżono karę umowną, Zamawiającemu przysługuje prawo dochodzenia odszkodowania na zasadach ogólnych Kodeksu cywilnego.
9. W przypadku wystąpienia okoliczności uzasadniających zapłatę przez Wykonawcę kar umownych, Zamawiający może według własnego wyboru potrącać kary umowne z ceny należnej Wykonawcy za wykonanie Umowy po uprzednim wezwaniu Wykonawcy do zapłaty kar umownych i bezskutecznym upływie wyznaczonego do zapłaty terminu, na co Wykonawca wyraża zgodę, wezwać Wykonawcę do zapłaty kar umownych w terminie 14 dni od daty otrzymania pisemnego wezwania do ich zapłaty lub skorzystać z zabezpieczenia należytego wykonania Umowy.
  10. W przypadku braku zapłaty lub nieterminowej zapłaty wynagrodzenia należnego podwykonawcom z tytułu zmiany wysokości wynagrodzenia odpowiadającego zmianom wskaźnika, o którym mowa w § 7 ust. 16 Umowy w zakresie dotyczącym zobowiązania podwykonawcy, Zamawiającemu przysługiwać będzie od Wykonawcy kara umowna w wysokości 1000,00 zł za każdy stwierdzony przypadek.
  11. Łączna wysokość kar umownych ze wszystkich tytułów wynikających z Umowy, zastrzeżonych na rzecz Zamawiającego jest ograniczona w stosunku do Wykonawcy do 80 % łącznej wartości Umowy netto wynikającej z § 7 ust. 1 Umowy.

#### **§ 9.**

##### **Prawa autorskie**

1. Wykonawca zapewnia, że korzystanie przez Zamawiającego z Projektu technicznego lub Dokumentacji powykonawczej nie będzie naruszało praw osób trzecich. Na podstawie Umowy Wykonawca przeniesie na Zamawiającego prawa majątkowe w zakresie i w sposób opisany poniżej.
2. Z dniem podpisania Protokołu odbioru Projektu technicznego lub Dokumentacji powykonawczej, o którym mowa w § 4 ust. 10 pkt 1 lub pkt 2 Umowy, Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do Projektu technicznego lub Dokumentacji powykonawczej, na polach eksploatacji wskazanych w ust. 3, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 1 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, użyczenie 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 rozporządanie i korzystanie na wszystkich polach eksploatacji wymienionych w pkt 1-4.
4. Z dniem dokonania przez Zamawiającego odbioru Projektu technicznego lub Dokumentacji powykonawczej, Zamawiający nabywa własność nośników, na których te utwory utrwalono, w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 1 Umowy.

#### **§ 10**

##### **Wady prawne**

1. Wykonawca gwarantuje, że dostarczony Sprzęt IT, Oprogramowanie, Projekt techniczny, Dokumenty oraz Dokumentacja powykonawcza nie naruszają praw własności intelektualnej ani innych praw osób trzecich.
2. W przypadku wystąpienia osób trzecich wobec Zamawiającego z roszczeniami opartymi na twierdzeniu, iż używany przez Zamawiającego Sprzęt IT, Oprogramowanie, Projekt techniczny, Dokumenty lub Dokumentacja powykonawcza naruszają jakiegokolwiek prawa, o których mowa w ust. 1, Zamawiającemu 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 Wykonawcy jakichkolwiek kosztów, odszkodowań itp.;
  - 2) prawo żądania zapłaty przez Wykonawcę 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 Zamawiającemu powództwa opartego na twierdzeniu opisanym w ust. 2, Wykonawca zobowiązuje się zapewnić Zamawiającemu na swój koszt ochronę sądową oraz ponieść konsekwencje zapadłego wyroku sądowego.



## § 11.

### Zabezpieczenie należytego wykonania Umowy (dalej „ZNWU”)

1. Wykonawca złożył u Zamawiającego ZNWU w jednej z form, o których mowa w art. 450 ust. 1 ustawy Prawo zamówień publicznych w wysokości \_\_\_\_\_,XX 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 % kwoty zabezpieczenia w terminie 30 dni od dnia podpisania bez zastrzeżeń przez upoważnionych przedstawicieli Stron Protokołu Odbioru, o którym mowa w § 4 ust. 7 Umowy;
  - 2) w wysokości 30 % kwoty zabezpieczenia w terminie 15 dni po upływie okresu Serwisu gwarancyjnego oraz rękojmi za wady Sprzętu IT.
4. W przypadku zmiany formy ZNWU w trakcie trwania Umowy obowiązywać będą poniższe zasady.
5. ZNWU w formie pieniężnej Wykonawca wpłaca przelewem na rachunek bankowy wskazany przez Zamawiającego.
6. ZNWU wnoszone w formie gwarancji bankowej lub ubezpieczeniowej może być wystawione przez bank albo ubezpieczyciela. Bank lub ubezpieczyciel zapłaci, na rzecz Zamawiającego w terminie 30 dni od pisemnego żądania kwotę \_\_\_\_\_,XX zł (słownie złotych: \_\_\_\_\_ XX/100), na pierwsze wezwanie Zamawiającego, bez odwołania, bez warunku, niezależnie od kwestionowania czy zastrzeżeń Wykonawcy i bez dochodzenia czy wezwanie Zamawiającego 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 \_\_\_\_\_,XX 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, Zamawiający 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 Wykonawcy.
10. ZNWU w formie innej niż pieniężna Wykonawca złoży u Zamawiającego w Kancelarii Głównej, Warszawa ul. Poleczki 33, z dopiskiem „Dla Departamentu Informatyki”. Zamawiający dopuszcza złożenie zabezpieczenia w formie gwarancji bankowej lub ubezpieczeniowej w formie dokumentu elektronicznego, opatrzonego kwalifikowanym podpisem elektronicznym.

## § 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 podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, Zamawiający może odstąpić od Umowy w terminie 30 (trzydziestu) dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego z tytułu wykonania części Umowy.
3. Przy wykonaniu Umowy Wykonawca bez pisemnej zgody Zamawiającego nie ma prawa do korzystania w jakimkolwiek charakterze z osób zatrudnionych u Zamawiającego, pod rygorem odstąpienia od Umowy przez Zamawiającego z winy Wykonawcy 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 Wykonawca jest zobowiązany do zapłaty w terminie 14 dni od wezwania przez Zamawiającego kary umownej w wysokości 20% łącznej kwoty brutto określonej w § 7 ust. 3 Umowy. Jeżeli szkoda poniesiona przez Zamawiającego jest wyższa od zastrzeżonej wyżej kary umownej, Zamawiający może dochodzić odszkodowania uzupełniającego od Wykonawcy na zasadach ogólnych Kodeksu cywilnego.

## § 13.

### Zawiadomienia

1. Wszelkie informacje wymienione lub niewymienione w Umowie (wyłącznie o charakterze techniczno – organizacyjnym), niezależnie od nazwy pod którą występują, dla swojej skuteczności muszą być przekazywane w formie pisemnej za zwrotnym, pisemnym potwierdzeniem odbioru i będą uważane za skutecznie doręczone w dniu ich odbioru, z zastrzeżeniem § 6 ust. 6 Umowy.
2. Zawiadomienia będą wysyłane na adresy i adresy poczty elektronicznej podane przez Strony. Każda ze Stron zobowiązana jest do informowania drugiej Strony o każdej zmianie podanego adresu lub adresu poczty elektronicznej

w formie pisemnej. Jeżeli Strona nie powiadomiła o zmianie adresu lub adresu poczty elektronicznej, zawiadomienia wysłane na ostatni znany adres lub adresu poczty elektronicznej, Strony uznają za doręczone.

3. Powiadomienia o powyższych zmianach nie stanowią zmiany Umowy wymagającej sporządzenia aneksu.

#### **§ 14.**

##### **Poufność i przetwarzanie danych osobowych**

1. Wszelkie informacje, w których posiadanie weszła druga Strona w związku z wykonywaniem Umowy są chronione. Każda ze Stron zobowiązuje się nie ujawniać ich osobom trzecim, także po zakończeniu Umowy, wyjąwszy przypadki przewidziane prawem.
2. Wykonawca zobowiązuje się do pisemnego zobowiązania osób realizujących Umowę do zachowania w poufności informacji, o których mowa w ust. 1.
3. Wykonawca zobowiązuje się do przestrzegania przy wykonywaniu Umowy przepisów Rozporządzeniu 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**”.
4. Wykonawca pisemnie zobowiąże pracowników realizujących zobowiązania określone w Umowie do przestrzegania przepisów, o których mowa w ust. 3.
5. Wykonawca oświadcza, że zapoznał się z klauzulami informacyjnymi w zakresie przetwarzania danych osobowych, stanowiącymi Załączniki nr 6a, 6c i 6d do Umowy, o ile znajdują zastosowanie.
6. Wykonawca 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. Wykonawca nie może bez zgody Zamawiającego przenieść praw wynikających z niniejszej Umowy na osoby trzecie.
2. Wszelkie postanowienia oraz zmiany treści Umowy wymagają formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu cywilnego, ustawy Prawo zamówień publicznych i ustawy o prawie autorskim i prawach pokrewnych.
4. Ewentualne spory mogące wyniknąć na tle wykonania Umowy rozstrzygać będzie sąd powszechny właściwy ze względu na siedzibę Zamawiającego.
5. Załączniki wymienione w Umowie stanowią jej integralną część:
  - 1) Załącznik nr 1 – Specyfikacja techniczna Sprzętu IT i Oprogramowania oraz zasady Wdrożenia;
  - 2) Załącznik nr 2 – Protokół odbioru – wzór
  - 3) Załącznik nr 3 – Protokół odbioru Projektu technicznego/ Dokumentacji powykonawczej – wzór
  - 4) Załącznik nr 4a – Protokół odbioru usunięcia wady (wzór)
  - 5) Załącznik nr 4b – Raport z przeprowadzonych konsultacji (wzór)
  - 6) Załącznik nr 5a – Załączniki 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 w zakresie przetwarzania danych osobowych, w przypadku bezpośredniego pozyskania danych Wykonawcy będącego osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą;
  - 9) Załącznik nr 6b – Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO (wzór);
  - 10) Załącznik nr 6c – Klauzula informacyjna w zakresie przetwarzania danych osobowych w przypadku pośredniego pozyskania danych osobowych pełnomocnika drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego/spółką cywilną;
  - 11) Załącznik nr 6d – Klauzula informacyjna w zakresie przetwarzania danych osobowych w przypadku bezpośredniego pozyskania danych osobowych pełnomocnika drugiej strony umowy będącej

osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego/spółką cywilną.

12) Załącznik nr 7 - Formularz ofertowy

13) Załącznik nr 8 – Wykaz osób

6. Umowę sporządzono w 4 (czterech) jednobrzmiących egzemplarzach, w tym jeden egzemplarz dla Wykonawcy i trzy egzemplarze dla Zamawiającego/Umowę sporządzono w formie elektronicznej i opatrzone kwalifikowanymi podpisami elektronicznymi przez upoważnionych przedstawicieli Stron.

**Wykonawca**

**Zamawiający**

.....

.....

.....

.....

W zależności od zaferowanych urządzeń przez Wykonawcę (urządzenia Firewall lub rozwiązanie równoważne) Zamawiający pozostawi w niniejszym Załączniku zapisy pkt. I lub pkt. II.

### Specyfikacja techniczna Sprzętu IT i Oprogramowania oraz zasady Wdrożenia

#### I. Urządzenia informatyczne pełniące funkcje zapory rdzenia Firewall – 2 szt., każde spełniające poniżej wskazane wymagania.

- 1.1. Zamawiający posiada w swojej infrastrukturze skonfigurowane zapory sieciowe Palo Alto PA-5250 oraz system zarządzania Panorama w związku z tym wymaga dostarczenia 2 sztuk urządzeń Palo Alto PA-5250 spełniających poniższe parametry techniczne (urządzenia będą działać w dwóch klastrach):
- 1.1.1. zaporą rdzenia PA-5250 wraz z zasilaczami AC - łącznie 2 sztuki,
  - 1.1.2. po 16 modułów 10GE SFP+ SR na każde urządzenie – łącznie 32 sztuki,
  - 1.1.3. po 4 moduły 10GE SFP+ SR dedykowanych dla przełączników HP 12910 FlexFabric (muszą być wspierane i kompatybilne z wymienionym urządzeniem) – łącznie 8 sztuk,
  - 1.1.4. 3 letnie licencje Threat prevention na każde urządzenie – łącznie 2 sztuki,
  - 1.1.5. 3 letnie licencje URL Filtering na każde urządzenie – łącznie 2 sztuki,
  - 1.1.6. 3 letnie licencje DNS Security na każde urządzenie – łącznie 2 sztuki,
  - 1.1.7. 3 letni support (Usługę Opieki Serwisowej) na każde urządzenie – łącznie 2 sztuki.

#### Zamawiający wymaga:

- 1.1. Aby wszystkie powyżej wskazane elementy (pkt. 1.1.1. – 1.1.7.) pochodziły od producenta posiadanego rozwiązania – Palo Alto.
- 1.2. Dostarczenia urządzeń z 36 miesięczną gwarancją producenta.
- 1.3. Wykonania Wdrożenia Sprzętu IT, zgodnie z zasadami określonymi w ppu wraz z załącznikami, stanowiącymi załącznik nr 7 do SWZ.
- 1.4. Wykonania Projektu technicznego i Dokumentacji powykonawczej w formie elektronicznej;
- 1.5. Świadczenia Serwisu gwarancyjnego dla Sprzętu IT (wraz ze wsparciem producenta), z czasem naprawy 6 godzin, przez okres 36 miesięcy na warunkach opisanych w ppu, stanowiących załącznik nr 7 do SWZ;
- 1.6. Oprogramowanie każdego z urządzeń realizujące wszystkie wymagane funkcje, jak też samo urządzenie musi być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowania np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania. Wszystkie funkcjonalności muszą być opublikowane na stronie producenta na dzień składania oferty.
- 1.7. Dostarczone urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, posiadać oznaczenie CE (zgodność z dyrektywami UE) oraz zapewniać gwarancję producenta dla użytkowników z obszaru Rzeczypospolitej Polskiej.
- 1.8. Aby zaferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia w okresie obowiązywania serwisu gwarancyjnego (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne).
- 1.9. Zamawiający wymaga oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie będą naruszały istniejącej gwarancji dla posiadanych urządzeń i Oprogramowania.
- 1.10. Zamawiający wymaga oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie naruszają istniejącej gwarancji oraz pochodzą z autoryzowanego kanału sprzedaży na rynek Polski.
- 1.11. Zapewnienie przez Wykonawcę 300 godzin konsultacji technicznych w okresie trwania Serwisu gwarancyjnego, jednak nie mniej niż 150 godzin. Konsultacje będą obejmowały analizy, audyty oraz rekomendacje 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.
- 1.12. W ramach konsultacji technicznych Wykonawca na wniosek Zamawiającego przeprowadzi warsztaty lub prezentacje dotyczące wskazanego elementu Sprzętu IT lub Oprogramowania w Centrali Zamawiającego przy ul. Poleczki 33 w Warszawie. Czas dojazdu do Zamawiającego nie będzie wliczony jako wykorzystanie dostępnej puli godzin.

Zamawiający dopuszcza przeprowadzenie konsultacji w formie zdalnej. Decyzję o formie przeprowadzenia konsultacji każdorazowo podejmie Zamawiający.

**II. Urządzenia równoważne**

1. W przypadku zaofiarowania rozwiązania równoważnego poprzez dostarczenie urządzeń zgodnych ze specyfikacją zawartą w Tabeli 1 zamieszczonej w pkt 4 poniżej. W przypadku zaofiarowania rozwiązania równoważnego Zamawiający wymaga spełnienia następujących wymagań:
  - 1.1. dostarczenie 4 urządzeń zgodnych z wymaganiami zawartymi w Tabeli 1 zamieszczonej w pkt 4 poniżej.
  - 1.2. dostarczenie systemu zarządzania opisanego w Tabeli 2 zamieszczonej w pkt 4 poniżej.
  - 1.3. dostarczenie licencji i Serwisu gwarancyjnego na 3 lata od odebrania dokumentacji powykonawczej.
  - 1.4. uruchomienie i wdrożenie przez Wykonawcę zapór rdzenia oraz przeniesie na nie polityki z eksploatowanych obecnie przez Zamawiającego zapór rdzenia (2 klastrów Check Point oraz 2 urządzeń Palo Alto PA-5250 - po dwa urządzenia w klastrze):
    - 1.4.1. proces wdrażania firewalli nie może spowodować przerwy dłuższej niż 2 godziny,
    - 1.4.2. wdrożenie musi się odbyć w przerwie serwisowej, której datę i godzinę wskaże Zamawiający na etapie uzgodnień z Wykonawcą.
- 1.2. uruchomienie i wdrożenie przez Wykonawcę Oprogramowania dla zapór rdzenia oraz przeniesie polityki, obiekty, logi (bezstratnie) z eksploatowanego obecnie przez Zamawiającego systemu Panorama:
  - 1.2.1. proces wdrażania systemu zarządzania nie może spowodować utraty logów,
  - 1.2.2. wdrożenie musi się odbyć w przerwie serwisowej, której datę i godzinę wskaże Zamawiający na etapie uzgodnień z Wykonawcą,
- 1.3. W przypadku zaofiarowania przez Wykonawcę rozwiązania równoważnego, Zamawiający wymaga dostarczenia wraz z ofertą kopii dokumentacji oferowanego systemu, publikowanej na ogólnie dostępnych stronach internetowych producenta, w której zaznaczy fragmenty wskazujące spełnienie poszczególnych wymagań równoważnych opisanych w tabelach 1 i 2. Muszą to być odwołania wprost do poszczególnych wymagań SWZ. Dokumentacja ta musi być w języku polskim. W przypadku, gdy producent na swoich stronach internetowych nie publikuje dokumentacji w języku polskim, Wykonawca dokona tłumaczenia z języka angielskiego. Za prawidłowość tłumaczenia odpowiada Wykonawca.
- 1.4. Zamawiający poniżej przedstawia wymagania równoważne dotyczące jednego urządzenia (poza wymaganiem Clientless VPN określonym w pkt. 11 w tabeli 1). Urządzenia będą działać w klastrze HA.

Tabela 1 - Minimalne wymagania równoważności dla urządzenia.

Nr	Wymagania minimalne
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". Wysokość maksymalnie 3U. Całość sprzętu musi być zarządzana przez jednego producenta.
2	Urządzenie musi być wyposażone w <ol style="list-style-type: none"> <li>1. 4 interfejsy 100/1000 Ethernet (RJ45)</li> <li>2. 16 interfejsów 1/10GE SFP+ obsadzone modułami 10GE SFP+ SR</li> <li>3. 4 porty 40GE/100GE QSFP+</li> </ol> UWAGA – wszystkie moduły (ilości) SFP/QSFP są podane dla jednego urządzenia
3	Urządzenie musi być wyposażone w dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w moduł Lights Out Management (LOM) lub odpowiednik pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania)
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: <ol style="list-style-type: none"> <li>1. Minimum 35 Gbps dla Firewall/kontroli aplikacji.</li> <li>2. Minimum 24 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware.</li> <li>3. Minimum 350 000 nowych połączeń na sekundę.</li> <li>4. Minimum 8 000 000 równoległych sesji.</li> </ol> <p>Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.</p> <p>Jako scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików</p>

	określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.
5	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy <ol style="list-style-type: none"> <li>1. rutera (tzn. w warstwie 3 modelu OSI),</li> <li>2. przełącznika (tzn. w warstwie 2 modelu OSI),</li> <li>3. w trybie pasywnego nasłuchu (sniffer).</li> </ol>
6	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)
7	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy na bazie, których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.
8	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
9	Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi, dla zapewnienia poufności i integralności danych, wykorzystywać TLS i IPsec..
10	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: <ol style="list-style-type: none"> <li>1. Minimum 18 Gbps dla IPSEC VPN.</li> <li>2. Minimum 4 000 tuneli IPSEC VPN (site-to-site).</li> <li>3. Minimum 30 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, Linux, MacOS, Android, iOS.</li> <li>4. Minimum 2 000 tuneli tzw. Clientless VPN - bez konieczności zastosowania klienta VPN.</li> </ol>
11	Funkcjonalność Clientless VPN, klienta VPN dla Linux, Android, iOS - Zamawiający wymaga dostarczenia licencji dla dwóch urządzeń w przypadku zaproponowania rozwiązania równoważnego,
12	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej <ol style="list-style-type: none"> <li>1. oznaczania pakietów znacznikami DiffServ,</li> <li>2. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego.</li> <li>3. utworzenia co najmniej 8 klas ruchu sieciowego.</li> <li>4. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.</li> <li>5. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego</li> </ol>
13	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
14	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
15	Urządzenie musi obsługiwać nie mniej niż 100 wirtualnych routerów posiadających odrębne tabele routingu.
16	Urządzenie musi obsługiwać nie mniej niż 25 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 100 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: <ol style="list-style-type: none"> <li>1. tablic routingu - minimum 5 per każda instancja. Jeżeli nie jest to możliwe, to dopuszcza się rozwiązania obsługujące 125 wirtualnych instancji firewall z obsługą jednej tablicy routingu per każda instancja.</li> <li>2. Polityk bezpieczeństwa obejmujących: <ol style="list-style-type: none"> <li>1) System IPS</li> <li>2) System ochrony antymalware/antyspyware</li> <li>3) System ochrony antywirus</li> </ol> </li> <li>3. Koncentratorów VPN dla zdalnego dostępu</li> </ol>
17	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.

18	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
19	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. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 60 000 reguł polityki bezpieczeństwa oraz obsługę minimum 15 000 stref bezpieczeństwa.
20	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
21	Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość” w polityce.
22	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
23	Urządzenie musi umożliwiać budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory, kondycja bezpieczeństwa stacji końcowej
24	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. Funkcja realizowana za pomocą profilu w ramach reguł bezpieczeństwa.
25	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
26	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download”.
27	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. Deszyfracja ruchu SSL będzie realizowana przed politykami bezpieczeństwa.
28	Urządzenie musi posiadać funkcję deszyfrowania ruchu TLS 1.2 i TLS 1.3 oraz wspierać protokół HTTP/2.
29	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
30	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: 1. Microsoft Active Directory, 2. usługi katalogowe LDAP, 3. serwery Terminal Services, 4. logi z syslog.
31	Urządzenie musi umożliwiać ustalić tożsamości użytkownika firewall poprzez aktywne uwierzytelnienie użytkownika z wykorzystaniem przeglądarki i captive portalu. Musi istnieć możliwość zdefiniowania co najmniej następujących rodzajów baz użytkowników dla captive portalu: 1. lokalna baza danych utrzymywana na firewallu. 2. zewnętrzna usługa katalogowa dostępna po LDAPS. 3. zewnętrzna usługa uwierzytelnienia i autoryzacji po RADIUS. Captive portal musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.

32	<p>Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet, gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.</p>
33	<p>Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa) Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi czy wsparcia producenta.</p> <p>Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
34	<p>Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekodery takie jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduły inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł AV musi wspierać protokół http/2.</p> <p>Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
35	<p>Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.</p> <p>Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
36	<p>Urządzenie NGFW musi umożliwiać granularną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa – nie dopuszcza się by IPS /lub AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego.</p>
37	<p>Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).</p> <p>Ochrona DNS co najmniej w zakresie</p> <ol style="list-style-type: none"> <li>1. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA).</li> <li>2. wykrywania nadużyć protokołu DNS w celu infiltracji i ekfiltracji danych.</li> <li>3. wykrywanie domen dynamicznych Dynamic DNS.</li> <li>4. wykrywanie zapytań do domen złośliwych, baza domen złośliwych musi posiadać co najmniej 10 milionów rekordów.</li> <li>5. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing).</li> </ol> <p>Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>



38	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
39	<p>Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering.</p> <p>Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL.</p> <p>Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).</p> <p>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.</p> <p>Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia na cały okres trwania gwarancji.</p>
40	Urządzenie musi posiadać funkcję ochrony przed atakami typu Zero-Day na bazie współpracy ze środowiskiem typu Sandbox. Wymagane jest, aby system pozwalał na przesyłanie do systemu Sandbox co najmniej plików wykonywalnych.
41	<p>Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW.</p> <p>Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).</p>
42	<p>1. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:</p> <p>1.1. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu.</p> <p>1.2. Operator, który ma możliwość tylko odczytu konfiguracji.</p> <p>2. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą</p> <p>2.1. bazy lokalnej,</p> <p>2.2. serwera LDAPS,</p> <p>2.3. RADIUS lub TACACS+</p> <p>2.4. SAML 2,0</p> <p>Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).</p>
43	Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
44	<p>Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia.</p> <p>Urządzenie musi mieć możliwość przywrócenia konfiguracji z określonego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.</p>
45	Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych. W szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
46	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. Musi istnieć możliwość przekierowania logowania różnych polityk bezpieczeństwa do różnych serwerów SYSLOG.
47	Urządzenie musi obsługiwać funkcjonalność typu Netflow, sFlow, jFlow itp.
48	Urządzenie musi być wyposażone w zasilacze typu AC Hot-Swap pracujące redundantnie.
49	Urządzenie musi być wyposażone w lokalną przestrzeń na logi o pojemności 2TB (przebieg użyteczna) działającej w RAID1
50	Urządzenie musi zostać dostarczone z 36 miesięczną gwarancją producenta.
51	Oprogramowanie każdego z urządzeń realizujące wszystkie wymagane funkcje jak też samo urządzenie musi być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania

	Wszystkie funkcjonalności muszą być opublikowane na stronie producenta na dzień składania oferty.
52	Dostarczone urządzenia muszą być fabrycznie nowe i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, posiadać oznaczenie CE (zgodność z dyrektywami UE) oraz zapewniać gwarancję producenta dla użytkowników z obszaru Rzeczypospolitej Polskiej.  Zamawiający wymaga oświadczenia producenta lub dystrybutora, że oferowane urządzenia nie będą naruszały istniejącej gwarancji dla posiadanych urządzeń i Oprogramowania.
53	Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia w najbliższym czasie (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne).

Tabela .2 – Minimalne wymagania równoważne dotyczące jednego systemu zarządzania.

Nr	Wymagania minimalne
1	Wraz z urządzeniami zapór rdzenia konieczne jest dostarczenie centralnego systemu zarządzania dostarczonego wraz z wszystkimi niezbędnymi elementami np. serwery, systemy operacyjne, systemy wirtualizacji
2	Urządzenia, na których będzie uruchomiony system zarządzania, logowania i raportowania, muszą spełniać co najmniej poniżej wskazane parametry tj.: 1. 16 CPU 2. 32 GB RAM 3. 24 TB przestrzeni dyskowej
3	System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne 1. obsługa nie mniej niż 20 firewalli fizycznych 2. obsługa nie mniej niż 1200 firewalli wirtualnych (w rozumieniu wirtualny kontekst/domena/system uruchomiony na dostarczonym firewallu) 3. obsługa co najmniej 10 000 logów/zdarzeń na sekundę 4. obsługa co najmniej 24 TB użytecznej przestrzeni dyskowej na logi
4	System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. 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 co najmniej 1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 2. tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. 3. tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych zapór rdzenia. 4. 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. 5. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”
6	System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej: 1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. >> Lokalnych (dla wybranych firewalli lub logicznych systemów firewalli) >> 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 firewalles w jednym, centralnym repozytorium. 5. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 6. Zarządzanie obiektami używanymi przez wszystkie firewalles w jednym, centralnym repozytorium 7. 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 co najmniej musi:

	<ol style="list-style-type: none"> <li>1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu,</li> <li>2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli,</li> <li>3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur,</li> <li>4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem,</li> <li>5. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów,</li> <li>6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone,</li> <li>7. informować o zmianach konfiguracji systemu.</li> </ol>
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.
9	Dostarczane zapory rdzenia, zapory brzegowe oraz system zarządzania muszą pochodzić od jednego producenta
10	System zarządzania, logowania i raportowania musi zostać dostarczony z 36 miesięcznym Serwisem gwarancyjnym.

**Wszystkie elementy opisane w Tabeli nr 1- Minimalne wymagania równoważności dla urządzenia oraz w Tabeli nr 2 – Minimalne wymagania równoważne dotyczące jednego systemu zarządzania muszą pochodzić od producenta oferowanego rozwiązania.**

**III. Zakres Projektu technicznego (dotyczy rozwiązania I albo II) – Projekt techniczny będzie zawierał co najmniej:**

1. Plan i harmonogram Wdrożenia;
2. Plan i harmonogram testów oraz procedury odbioru Wdrożenia;
3. Docelową architekturę sieci po wykonaniu wdrożenia w obszarze bramki internetowej Zamawiającego (schematy połączeń fizycznych i logicznych sieci zarządzającej LAN wraz z adresacją oraz schematy połączeń fizycznych i logicznych Sprzętu IT uwzględniające posiadaną już infrastrukturę LAN Zamawiającego z podziałem zgodnie z konfiguracją na urządzeniach IT posiadanych przez Zamawiającego);
4. Sposób migracji z platformy Check Point oraz w przypadku rozwiązania równoważnego Palo Alto,
5. Nazwy modeli, numery seryjne Sprzętu IT oraz nazwy, wersje licencji Oprogramowania i firmware'u;

**IV. Wdrożenie (dotyczy rozwiązania I albo II) - w ramach Wdrożenia Wykonawca wykona co najmniej następujące czynności:**

1. Wdrożenie zostanie wykonane zgodnie z zakresem określonym w odebrany przez Zamawiającego Projekcie technicznym;
2. Zainstaluje Sprzęt IT i Oprogramowanie w COPD (rack 19"), we wskazanym przez Zamawiającego miejscu, przy czym instalacja obejmuje dostawę i montaż kabli logicznych i zasilających;
3. Uruchomi i wdroży dostarczane zapory rdzenia oraz przeniesie na nie polityki z eksploatowanych obecnie przez Zamawiającego zapór rdzenia składającego się z dwóch klastrów Check Point oraz w przypadku zaproponowania rozwiązania równoważnego 2 urządzeń Palo Alto - po dwa urządzenia w klastrze;
4. W przypadku zaproponowania rozwiązania równoważnego zainstaluje uruchomi i wdroży Oprogramowanie dla zapór rdzenia będące systemem zarządzania wraz ze wszystkimi dostarczonymi elementami wchodzącymi w jego skład oraz przeniesie polityki, obiekty, logi (bezzstrasznie) z eksploatowanego obecnie przez Zamawiającego systemu Panorama;
5. Podłączy Sprzęt IT do sieci zasilającej i sieci logicznej, zainstaluje Oprogramowanie oraz skonfiguruje w sposób umożliwiający uzyskanie przez Zamawiającego dostępu do kompletnie skonfigurowanych oraz widocznych dla administratora zasobów Sprzętu IT z poziomu GUI;
6. Uruchomi Sprzęt IT oraz przedstawi, na życzenie Zamawiającego, poszczególne lub wszystkie funkcjonalności Sprzętu IT i Oprogramowanie, o których mowa w niniejszym Załączniku oraz w Załączniku nr 7 do Umowy;
7. Przygotuje konfigurację Sprzętu IT (konfiguracja klastra rozciągniętego na dwie lokalizacje);
8. Dokona migracji z klastra Check Point i w przypadku zaproponowania rozwiązania równoważnego również klastra Palo Alto wraz z przeniesieniem wszystkich funkcji zaimplementowanych na ww. urządzeniach;
9. Uruchomi i zaprezentuje w celach testowych wybrane przez Zamawiającego funkcjonalności;
10. Zainstaluje Sprzęt IT i skonfiguruje Oprogramowanie w COPD;
11. W przypadku wdrożenia urządzeń Palo Alto zaktualizuje obecnie pracujący klastr Palo Alto do dostarczanej wersji firmware;
12. Uruchomi Sprzęt IT produkcyjnie z funkcjonalnościami wskazanymi przez Zamawiającego;
13. Dokona instruktażu obsługi wdrożonego Sprzętu IT dla 10 pracowników Zamawiającego, czas trwania instruktażu wyniesie do 5 Dni Roboczych.
14. Wykona testy wdrożonej konfiguracji polegające na sprawdzeniu poprawności komunikacji wszystkich Urządzeń IT podłączonych poprzez Sprzęt IT;
15. Sposób wykonania instalacji:

- 15.1. Zamawiający posiada gniazda zasilające typu 2P+Z w szafach dedykowanych dla dostarczanego Sprzętu IT. W ramach Umowy w przypadku dostawy Sprzętu IT wymagającego innego sposobu zasilania musi być zrealizowane wykonanie obwodów doprowadzających zasilanie do Sprzętu IT (szacunkowa długość kabli zasilających do 25 metrów). Z uwagi na brak informacji jakie jest wymagane zasilanie dla dostarczanych (min. ilość obwodów, typ wtyków zasilających dla Sprzętu IT) Zamawiający nie jest w stanie przygotować infrastruktury zasilającej dla proponowanego rozwiązania niż obecnie posiadana.
- 15.2. W szafach Zamawiającego przewidziane jest wolne miejsce na zamawiany Sprzęt IT więc nie ma konieczności demontażu lub relokacji innych urządzeń.
- 15.3. Wykonawca zobowiązany jest dostarczyć odpowiednie kable łączące z siecią LAN oraz kable zasilające.
- 15.4. Zamawiający nie określa dokładnej ilości kabli LAN i zasilających, ilość powinna wynikać ze specyfiki dostarczonego Sprzętu IT.
- 15.5. Standard dostarczanych kabli: światłowody min. OM4, przewody miedziane min. kat.6 (odpowiednie do zaproponowanego rozwiązania).

**Protokół odbioru - wzór**

zgodnie z Umową nr ..... zawartą pomiędzy:  
 Agencją Restrukturyzacji i Modernizacji Rolnictwa („Zamawiającym”) a  
 ..... („Wykonawcą”),  
 Zamawiający potwierdza, że Wykonawca dostarczył Sprzęt i Oprogramowanie wymienione w Specyfikacji Technicznej:

Lp.	Nazwa Sprzętu i Oprogramowania	Liczba (szt.)	Numer seryjny / Uwagi
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Upoważnieni przedstawiciele Zamawiającego i Wykonawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że:

- Dostarczony do Lokalizacji Zamawiającego Sprzęt jest fabrycznie nowy i nie nosi śladów uszkodzeń zewnętrznych oraz uprzedniego używania.
- Liczba i rodzaj dostarczonego do Lokalizacji Zamawiającego Sprzętu oraz Oprogramowania jest zgodna z Umową (w tym z Załącznikami nr 1 i 2 oraz 4 do Umowy).
- Wraz ze Sprzętem do Lokalizacji Zamawiającego dostarczono wymaganą Dokumentację.
- Dostarczony Sprzęt oraz Oprogramowanie narzędziowe są wolne od oprogramowania szkodliwego i szpiegującego, a także są zabezpieczone przed nieautoryzowanym dostępem.

Uwagi i zastrzeżenia:

Zamawiający - Lokalizacja Zamawiającego (upoważniony przedstawiciel)		Wykonawca (upoważniony przedstawiciel)
.....		.....
.....		.....

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

**Protokół odbioru Projektu technicznego/ Dokumentacji powykonawczej -wzór**

Dane dokumentu:

Nazwa projektu:  Lokalizacja:  Wykonawca:
Data dokumentu:  Lista wersji

Uwagi :

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

Zamawiający odbiera / nie odbiera\* Projekt techniczny/ Dokumentację powykonawczą\*

Zamawiający - Lokalizacja Zamawiającego <i>(upoważniony przedstawiciel)</i>			Wykonawca <i>(upoważniony przedstawiciel)</i>
.....			.....
.....			.....
....., dnia ..... roku			

\* niepotrzebne skreślić

Załącznik nr 4a do Umowy nr \_\_\_\_/DI/2021/2610

**Protokół odbioru usunięcia wady (wzór)**

1. Imiona i nazwiska osób dokonujących czynności odbioru:

2. Opis czynności wykonanych w ramach usunięcia wady:

3. Data podpisania protokołu

4. Podpisy

Załącznik nr 4b do Umowy nr \_\_\_\_/DI/2021/2610

**Raport z przeprowadzonych konsultacji (wzór)**

1. Opis konsultacji w kwartale..... (data)

.....  
.....  
.....  
.....

2. ilość wykorzystanych godzin konsultacji .....

3. Uwagi/ zastrzeżenia

4. Podpisy i data

Wykonawca

Zamawiający



Załącznik nr 5a do Umowy nr \_\_\_\_/DI/2021/2610

**Załączniki 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 5b do Umowy nr \_\_\_\_/DI/2021/2610

**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.**

Wykonawca 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.

.....  
(data, podpis osoby upoważnionej, pieczęć)

**Klauzula informacyjna w zakresie przetwarzania danych osobowych<sup>1</sup>**

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) oraz przepisów krajowych wydanych w związku z ogólnym rozporządzeniem o ochronie danych, zwanym dalej: „**RODO**”, dalej: „**RODO**” Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II nr 70, 00-175 Warszawa. Z Administratorem można kontaktować się poprzez e-mail: [info@arimr.gov.pl](mailto:info@arimr.gov.pl) lub pisemnie na adres korespondencyjny Centrali Agencji Restrukturyzacji i Modernizacji Rolnictwa: ul. Poleczki 33, 02-822 Warszawa.
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](mailto:iod@arimr.gov.pl) lub pisemnie na adres korespondencyjny Administratora, wskazany w pkt 1.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
  - 1) organy kontrolne,
  - 2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020, poz. 2176),
  - 3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
  - 4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, 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 będzie 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 będzie przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia, prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych oraz prawo do przenoszenia Pani/Pana danych osobowych, w przypadkach określonych w RODO.
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.

<sup>1</sup> Niniejsza klauzula w zakresie przetwarzania danych osobowych znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą.

**Oświadczenie o wypełnieniu obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO**

..... 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 „Wykonawcą”

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO<sup>2</sup> wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu zawarcia oraz wykonania Umowy<sup>3</sup>.

(podpisy)

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

<sup>2</sup> Rozporządzeniu 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).

<sup>3</sup> W przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa.

**Klauzula informacyjna w zakresie przetwarzania danych osobowych<sup>4</sup>**

W związku z treścią z art. 14 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. U.UE.L 2016.119. z 04.05.2016 r., s. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., s. 2.) dalej: „RODO” Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II nr 70, 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.
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.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu zawarcia oraz wykonania niniejszej umowy.
4. Administrator będzie przetwarzał następujące kategorie Pani/Pana danych: dane identyfikacyjne oraz dane kontaktowe.
5. Odbiorcami Pani/Pana danych osobowych mogą być:
  - 1) organy kontrolne,
  - 2) osoby lub podmioty, którym Administrator udzielił informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 poz. 2176),
  - 3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
  - 4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, m. in. dostawcy IT.
6. Pani/Pana dane osobowe będą przechowywane przez okres obowiązywania umowy, zawartej z Agencją Restrukturyzacji i Modernizacji Rolnictwa. Okres przechowywania danych będzie 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 będzie przedłużony na okres 5 lat, na potrzeby archiwizacji.
7. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
8. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. Pani/Pana dane Administrator uzyskał od firmy [...\*].

\*należy wskazać źródło pozyskania danych [nazwę firmy, od której Administrator pozyskał dane].

<sup>4</sup> Niniejsza klauzula w zakresie przetwarzania danych osobowych, znajdzie zastosowanie w przypadku pośredniego pozyskania danych pełnomocników drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego/ spółką cywilną.

**Klauzula informacyjna w zakresie przetwarzania danych osobowych<sup>5</sup>**

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. U.UE.L 2016.119. z 04.05.2016 r., s. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., s. 2.), dalej: „RODO” Zamawiający informuje, że:

1. Administratorem Pani/Pana danych osobowych (dalej: Administrator) pozyskanych w związku z zawarciem umowy jest Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie, Al. Jana Pawła II nr 70, 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.
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.
3. Dane osobowe pozyskane przez Administratora przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu zawarcia oraz wykonania niniejszej umowy.
4. Odbiorcami Pani/Pana danych osobowych mogą być:
  - 1) organy kontrolne,
  - 2) osoby lub podmioty, którym Administrator udzieli informacji publicznej zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 poz. 2176),
  - 3) podmioty uprawnione do przetwarzania danych osobowych na podstawie przepisów powszechnie obowiązującego prawa,
  - 4) podmioty przetwarzające w imieniu Administratora na mocy zawartej umowy, 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 będzie 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 będzie przedłużony na okres 5 lat, na potrzeby archiwizacji.
6. Przysługuje Pani/Panu prawo do dostępu do Pani/Pana danych osobowych, ich sprostowania, usunięcia oraz prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych, w przypadkach określonych w RODO.
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.

<sup>5</sup> Niniejsza klauzula w zakresie przetwarzania danych osobowych, znajdzie zastosowanie w przypadku bezpośredniego pozyskania danych pełnomocnika drugiej strony umowy będącej osobą fizyczną/osobą fizyczną prowadzącą działalność gospodarczą oraz reprezentantów drugiej strony umowy będącej spółką prawa handlowego/ spółką cywilną.

Załącznik nr 7 do Umowy nr \_\_\_\_/DI/202.../2610

**Formularz ofertowy**

Załącznik nr 8 do Umowy nr \_\_\_\_/DI/202..../2610

**Wykaz osób**



**Załącznik nr 7 do SWZ – 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 SWZ\_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 Urzędu, należy wybrać „pl Polski”, a w dalszej kolejności zaznaczyć „Jestem wykonawcą”. Następnie należy zaimportować „ESPD” wczytując plik w formacie XML będący Załącznikiem nr 7 do SWZ. Po sporządzeniu oświadczenia w formie jednolitego europejskiego dokumentu zamówienia („*JEDZ*”) należy je podpisać przez osobę lub osoby uprawnione.

Aktualne na dzień składania ofert oświadczenie w formie JEDZ należy złożyć w formie elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, za pomocą środka komunikacji elektronicznej, tj. Platformę Zakupową. Szczegółowy zakres wymagań określony został w Rozdz. IV.2 SWZ.

