Zamawiający:

**Sąd Okręgowy w Warszawie**
**al. „Solidarności” 127**
**00-898 Warszawa**

**PRZETARG NIEOGRANICZONY**

na:

# „Usługę zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego”

**ZP/OI/27/18**

## SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r.
Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r. poz. 1579 ze zm.)

**WARSZAWA – PAŹDZIERNIK 2018 r.**

**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA (SIWZ)**

## ROZDZIAŁ I. INFORMACJE WSTĘPNE

### 1. Zamawiający:

Sąd Okręgowy w Warszawie
Adres: 00-898 Warszawa, al. „Solidarności" 127
Godziny urzędowania: poniedziałek – piątek od godz. 8.00 do godz. 16.00.
NIP: 527-20-26-252, Regon: 000324694
http://bip.warszawa.so.gov.pl/

### 2. Postępowanie prowadzi:

Samodzielna Sekcja ds. Zamówień Publicznych Sądu Okręgowego w Warszawie
Adres: 00-898 Warszawa, al. „Solidarności" 127
Fax: 22 440 50 42
e-mail: rzp@warszawa.so.gov.pl

Postępowanie, którego dotyczy niniejszy dokument, oznaczone jest znakiem:

**ZP/OI/27/18**

Wykonawcy we wszelkich kontaktach z zamawiającym powinni powoływać się na ten znak.

### 3. Tryb postępowania

1) Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie przetargu nieograniczonego, zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r. poz. 1579 ze zm.), zwaną dalej „ustawą", o wartości szacunkowej zamówienia nieprzekraczającej wyrażonej w złotych równowartości kwoty 144.000 euro.
2) W kwestiach nieuregulowanych w specyfikacji istotnych warunków zamówienia zastosowanie mają przepisy powyższej ustawy oraz przepisy aktów wykonawczych do niej.

### 4. Informacje ogólne

1) Wszelką pisemną korespondencję do zamawiającego związaną z niniejszym postępowaniem należy kierować na adres: Samodzielna Sekcja ds. Zamówień Publicznych Sądu Okręgowego w Warszawie, al. „Solidarności" 127, 00–898 Warszawa. W przypadku osobistego złożenia korespondencji przez wykonawcę należy złożyć ją na Biurze Podawczym znajdującym się na parterze w pokoju nr 14.
2) Porozumiewanie się zamawiającego z wykonawcami odbywa się drogą pisemną z dopuszczeniem możliwości przekazywania wniosków, zawiadomień i informacji drogą elektroniczną na adres e-mail: rzp@warszawa.so.gov.pl.
3) Jeżeli zamawiający lub wykonawca przekazują, wnioski, zawiadomienia oraz informacje drogą elektroniczną lub faxem, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
4) W ramach niniejszego postępowania wszelka korespondencja prowadzona jest w języku polskim.
5) Osobą upoważnioną do bezpośredniego kontaktu z wykonawcami ze strony zamawiającego jest Pani Magdalena Polubiec.

## ROZDZIAŁ II. PRZEDMIOT I TERMIN REALIZACJI ZAMÓWIENIA

### 1. Przedmiot zamówienia

1) Przedmiotem zamówienia jest świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego dla Sądu Okręgowego w Warszawie za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach zamawiającego:
   - al. „Solidarności" 127 w Warszawie,
   - ul. Czerniakowskiej 100 w Warszawie,
   - ul. Płockiej 9 w Warszawie.
2) Szczegółowy opis przedmiotu zamówienia stanowi Załącznik Nr 1 do specyfikacji istotnych warunków zamówienia.
3) Przedmiot zamówienia będzie realizowany zgodnie z postanowieniami projektu umowy, stanowiącego Załącznik Nr 6 do specyfikacji istotnych warunków zamówienia.
4) Zamawiający nie przewiduje możliwości udzielenia wykonawcy zamówień uzupełniających na podstawie art. 67 ust. 1 pkt 6 ustawy.
5) Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej.
6) Zamawiający nie dopuszcza składania ofert wariantowych.
7) Zamawiający nie dopuszcza składania ofert częściowych.
8) Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy, z zastrzeżeniem pkt 9-10. Wykonawca zobowiązany jest do wskazania w ofercie części zamówienia, której wykonanie zamierza powierzyć podwykonawcy i podania przez wykonawcę firm podwykonawców.
9) W przypadku zamówień na usługi, które mają być wykonane w miejscu podlegającym bezpośredniemu nadzorowi zamawiającego, zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia wykonawca, o ile są już znane, podał nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w takie usługi. Wykonawca zawiadamia zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację usług.
10) Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
11) Przedmiot zamówienia zgodnie ze Wspólnym Słownikiem Zamówień - kod CPV:
    32420000-3 – urządzenia sieciowe.

### 2. Wymagany termin wykonania zamówienia

Przedmiot zamówienia realizowany będzie dwuetapowo:
1) I etap – zapewnienie usługi zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy- 30 dni od dnia podpisania umowy,
2) II etap - zapewnienie wsparcia technicznego przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM- 36 miesięcy od dnia zakończenia I etapu.

## ROZDZIAŁ III. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

### 1. Informacje ogólne

1) Każdy wykonawca może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty wariantowej spowoduje odrzucenie wszystkich ofert złożonych przez wykonawcę.
2) Oferta musi obejmować cały przedmiot zamówienia.
3) Wszelkie koszty związane z przygotowaniem oraz dostarczeniem oferty ponosi wykonawca.

### 2. Wymagania formalne dotyczące oferty

1) Ofertę można złożyć jedynie w formie pisemnej przy użyciu nośnika pisma nieulegającego usunięciu bez pozostawienia śladów.
2) Oferta wraz z załącznikami musi być przygotowana w języku polskim.
3) Dokumenty sporządzone w języku obcym należy złożyć wraz z ich tłumaczeniem na język polski.

4) Zamawiający zastrzega, że w przypadku wskazania przez wykonawcę dostępności oświadczeń lub dokumentów potwierdzających spełnianie przez wykonawcę warunków udziału w postępowaniu oraz potwierdzających brak podstaw wykluczenia wykonawcy z udziału w postępowaniu, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, a pobranych samodzielnie przez zamawiającego, wykonawca na wezwanie zamawiającego przedstawi tłumaczenia niniejszych dokumentów.
5) Każda zapisana strona oferty musi być podpisana przez wykonawcę (podpis i pieczątka imienna lub czytelny podpis). Również wszystkie załączniki do oferty (każda zapisana strona) stanowiące oświadczenia wykonawcy, a także wszelkie miejsca, w których wykonawca naniósł zmiany muszą być podpisane przez wykonawcę i dodatkowo opatrzone datą dokonania poprawki.
6) W przypadku, gdy wykonawcę reprezentuje pełnomocnik, do oferty musi być załączone pełnomocnictwo w oryginale określające jego zakres lub notarialnie poświadczona kopia.
7) Dla celów porządkowych, wszystkie strony oferty należy kolejno ponumerować i uzyskaną liczbę wpisać do formularza oferty. Wszystkie strony oferty powinny być spięte lub zszyte w sposób zabezpieczający przed jej dekompletacją.
8) W przypadku, gdyby oferta lub składane wraz z nią dokumenty zawierały informacje, stanowiące tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, wykonawca powinien w sposób niebudzący wątpliwości zastrzec, nie później niż w terminie składania ofert, które spośród przedstawionych informacji stanowią tajemnicę przedsiębiorstwa i nie mogą być udostępniane. Informacje te powinny być umieszczone w osobnym wewnętrznym opakowaniu, trwale ze sobą połączone i ponumerowane, z zachowaniem ciągłości numeracji stron oferty. Nie mogą stanowić tajemnicy przedsiębiorstwa informacje podawane do wiadomości podczas otwarcia ofert, tj. nazwa (firma) oraz adres wykonawcy, informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofercie.
   W przypadku dokonania zastrzeżenia wykonawca zobowiązany jest załączyć do oferty uzasadnienie podstaw faktycznych i prawnych zastrzeżenia jako tajemnicy przedsiębiorstwa określonych informacji. Niezałączenie uzasadnienia będzie świadczyło o nieodpowiednim zastrzeżeniu tajemnicy przedsiębiorstwa, co skutkować będzie odtajnieniem zastrzeżonych elementów oferty.

### 3. Zawartość merytoryczna oferty

Oferta powinna być sporządzona na formularzu ofertowym, stanowiącym Załącznik Nr 2 do specyfikacji istotnych warunków zamówienia i zawierać cenę ofertową wykonania przedmiotu zamówienia, wyliczoną w sposób określony w Rozdziale VI ust. 5 specyfikacji istotnych warunków zamówienia. Jednocześnie cena ta powinna być wyliczona w oparciu o szczegółowy opis przedmiotu zamówienia, stanowiący Załącznik Nr 1 do specyfikacji istotnych warunków zamówienia, z uwzględnieniem warunków wykonania przedmiotu zamówienia, określonych w projekcie umowy, stanowiącym Załącznik Nr 6 do specyfikacji istotnych warunków zamówienia.

### 4. Sposób opakowania i dostarczenia oferty

1) Ofertę (formularz oferty wraz z wymaganymi załącznikami) należy składać w nieprzejrzystym i zamkniętym opakowaniu. Opakowanie powinno być odpowiednio zabezpieczone w sposób uniemożliwiający bezśladowe otworzenie (np. podpisane na wszystkich połączeniach).
2) Opakowanie powinno być zaadresowane do zamawiającego na adres:

Sąd Okręgowy w Warszawie
Samodzielna Sekcja ds. Zamówień Publicznych
00-898 Warszawa, al. „Solidarności” 127

z dopiskiem:
„OFERTA DO PRZETARGU”

**„Usługa zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego”**

**numer zamówienia ZP/OI/27/18**

3) Opakowanie powinno być opatrzone pełną nazwą i dokładnym adresem wykonawcy składającego daną ofertę (ulica, numer lokalu, miejscowość, numer kodu pocztowego).
4) Zmiana lub wycofanie oferty dokonane przez wykonawcę przed upływem terminu do składania ofert są skuteczne, przy czym:
   a) zmiany dotyczące treści oferty powinny być przygotowane, opakowane i zaadresowane w ten sam sposób co oferta. Ponadto opakowanie, w którym jest przekazywana zmieniona oferta należy opatrzyć napisem „ZMIANA";
   b) powiadomienie o wycofaniu oferty powinno być opakowane i zaadresowane w ten sam sposób co oferta. Ponadto opakowanie, w którym jest przekazywane to powiadomienie należy opatrzyć napisem „WYCOFANIE".

## ROZDZIAŁ IV. BRAK PODSTAW DO WYKLUCZENIA ORAZ DOKUMENTY POWIERDZAJĄCE, ZE OFEROWANE USŁUGI SPEŁNIAJĄ WYMAGANIA OKREŚLONE PRZEZ ZAMAWIAJACEGO

### 1. Brak podstaw do wykluczenia.

O udzielenie zamówienia ubiegać się mogą wykonawcy, wobec których brak jest podstaw do wykluczenia z postępowania o udzielenie zamówienia z powodu niespełniania warunków, o których mowa w art. 24 ust. 1 ustawy.

### 2. Oświadczenia i dokumenty potwierdzające spełnianie warunków udziału w postępowaniu, o których mowa w ust. 1 oraz brak podstaw do wykluczenia wykonawcy z powodu niespełniania warunków, o których mowa w art. 24 ust. 1 ustawy.

2.1 Każdy wykonawca zobowiązany jest do złożenia wraz z ofertą oświadczenia o braku podstaw do wykluczenia z postępowania, na formularzu stanowiącym Załącznik Nr 4 do specyfikacji istotnych warunków zamówienia.
2.2 W terminie 3 dni od zamieszczenia przez zamawiającego informacji na stronie internetowej, o której mowa w art. 86 ust. 5 ustawy, każdy wykonawca zobowiązany jest do złożenia oświadczenia o przynależności lub braku przynależności do tej samej grupy kapitałowej, do której należą inni wykonawcy, którzy złożyli odrębne oferty, na formularzu stanowiącym Załącznik Nr 5 do specyfikacji istotnych warunków zamówienia. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
2.3 Wszystkie dokumenty muszą być złożone w formie oryginału lub w formie kopii poświadczonej za zgodność z oryginałem odpowiednio przez wykonawcę, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcę wspólnie ubiegającego się o udzielenie zamówienia publicznego, w zakresie dokumentów, które każdego z nich dotyczą (każda zapisana strona), za wyjątkiem oświadczenia dotyczącego wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a ustawy, które składane są tylko w oryginale.
2.4 Zamawiający zażąda przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu, gdy złożona kopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jej prawdziwości.
2.5 Zamawiający w tym postępowaniu przewiduje stosowanie procedury określonej w art. 24 aa ustawy, tj. może dokonać najpierw oceny ofert, a następnie zbadać, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu. Jeżeli wykonawca uchyla się od zawarcia umowy, zamawiający może zbadać, czy nie podlega wykluczeniu wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert.
2.6 Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, zamawiający może na każdym etapie postępowania wezwać wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie

podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.

**3. Warunki dotyczące przedmiotu zamówienia**

1) W celu potwierdzenia, że oferowane usługi odpowiadają wymaganiom określonym przez zamawiającego w Szczegółowym opisie przedmiotu zamówienia, stanowiącym Załącznik Nr 1 do SIWZ zamawiający wymaga:
   a) aby Wykonawca złożył dokument pochodzący od importera technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
   b) złożenia oświadczenia producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
2) Ww. dokumentów zamawiający będzie żądał od wykonawcy, którego oferta w ocenie zamawiającego została najwyżej oceniona.

**5. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia**

W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, dokumenty o których mowa w ust. 2 pkt 2.1 i 2.2 składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje brak podstaw wykluczenia.

## ROZDZIAŁ V. WADIUM

Zamawiający nie wymaga wniesienia wadium.

## ROZDZIAŁ VI. OPIS SPOSOBU OBLICZENIA CENY

1. Cena powinna zostać wyrażona cyfrowo i słownie.
2. Cenę należy podać w złotych polskich do dwóch miejsc po przecinku. Wszelkie rozliczenia dotyczące realizacji zamówienia dokonywane będą w złotych polskich. Zamawiający nie przewiduje możliwości dokonywania rozliczeń z wykonawcą w walutach obcych.
3. Poszczególne ceny wskazane w ofercie muszą być skalkulowane rzetelnie i w sposób jednoznaczny.
4. Cena oferty musi uwzględniać wszystkie koszty niezbędne do zrealizowania przedmiotu zamówienia wynikające ze szczegółowego opisu przedmiotu zamówienia, stanowiącego Załącznik Nr 1 do specyfikacji istotnych warunków zamówienia, a bez których nie można wykonać przedmiotu zamówienia oraz uwzględniać warunki realizacji przedmiotu zamówienia opisane w projekcie umowy, stanowiącym Załącznik Nr 6 do specyfikacji istotnych warunków zamówienia.
5. Cena za realizację przedmiotu zamówienia nie będzie podlegała waloryzacji. Cena jest stała do końca trwania umowy z zastrzeżeniem zapisów Rozdziału X specyfikacji istotnych warunków zamówienia.
6. Wykonawca zobowiązany jest do wyliczenia i wskazania całkowitej ceny realizacji zamówienia z podatkiem VAT w okresie trwania umowy. W ust. 1 Formularza ofertowego, stanowiącym Załącznik Nr 2 do specyfikacji istotnych warunków zamówienia należy wpisać kwotę, w oparciu o sumę cen z podatkiem VAT, podanych w ust. 1 pkt. 1 i 2 Formularza ofertowego obliczoną odpowiednio dla I etapu i II etapu realizacji umowy. Wartość etapu I stanowi 70% całkowitej ceny z podatkiem VAT podanej w ust. 1 Formularza ofertowego. Wartość etapu II realizacji umowy stanowi 30% całkowitej ceny z

podatkiem VAT podanej w ust. 1 Formularza ofertowego. W celu wyliczenia ceny dla etapu II należy cenę miesięcznego wynagrodzenia za świadczenie usługi wsparcia technicznego pomnożyć przez ilość świadczeń usługi, tj. 36 miesięcy. Kwotę z podatkiem VAT wpisać w ust. 1 Formularza ofertowego. Od kwoty z podatkiem VAT należy wyliczyć kwotę bez podatku VAT, stawka VAT wynosi 23%.
Określenie wartości poszczególnych etapów na innym poziomie niż 70% i 30% traktowane będzie jako błąd w obliczaniu ceny.

## ROZDZIAŁ VII. TERMINY

### 1. Termin związania ofertą

1) Wykonawca składający ofertę pozostaje nią związany przez okres 30 dni.
2) Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

### 2. Termin składania i otwarcia ofert

1) Oferty należy składać na Biurze Podawczym Sądu Okręgowego w Warszawie, 00-898 Warszawa, al. „Solidarności" 127, pokój nr 14, w terminie **do dnia 22 października 2018 r. do godz. 12:00**, pod rygorem zwrotu bez otwierania oferty złożonej po tym terminie, bez względu na przyczyny opóźnienia.
2) Dopuszczalne jest składanie ofert drogą pocztową z zastrzeżeniem, że decyduje data i godzina dostarczenia przesyłki na wskazany w pkt 1 adres zamawiającego, a nie data stempla pocztowego (nadania).
3) Otwarcie ofert odbędzie się **w dniu 22 października 2018 r. o godz. 12:30** w Samodzielnej Sekcji ds. Zamówień Publicznych Sądu Okręgowego w Warszawie, 00-898 Warszawa, al. „Solidarności" 127, pokój513.

## ROZDZIAŁ VIII. KRYTERIA I SPOSÓB OCENY OFERT

1) Zamawiający oceni i porówna jedynie te oferty, które nie zostały odrzucone.
2) Kryteriami oceny ofert są:
   a) cena ofertowa - waga kryterium 60%,
   b) najkrótszy czas reakcji na zgłoszenie serwisowe – waga kryterium 20%,
   c) najkrótszy czas na podjęcie działań serwisowych od chwili reakcji na zgłoszenie serwisowe – waga kryterium 20%.

3) Ocena ofert będzie dokonywana w zakresie każdego kryterium w następujący sposób:

   a) cena ofertowa:

   Liczba punktów, którą można uzyskać w ramach tego kryterium, zostanie obliczona wg wzoru:

$$C = \frac{Cmin}{Ci} x100x60\%$$

   gdzie:
   C - liczba punktów za cenę ofertową
   $C_{min}$- najniższa proponowana cena
   $C_i$ - cena oferty badanej,

   b) najkrótszy czas reakcji na zgłoszenie serwisowe (R):

   Liczba punktów, którą można uzyskać w ramach tego kryterium, zostanie obliczona wg wzoru:

$$R = \frac{Rmin}{Ri} x100x20\%$$

gdzie: R- liczba punktów za najkrótszy termin reakcji na zgłoszenie serwisowe,
$R_{min}$ – najkrótszy czas reakcji na zgłoszenie serwisowe,
$R_i$ – czas reakcji na zgłoszenie serwisowe wskazany w badanej ofercie.

Punkty w przedmiotowym kryterium zostaną przyznane jedynie temu wykonawcy, który w Formularzu ofertowym wskaże oferowany czas reakcji na zgłoszenie serwisowe. Przy czym zamawiający przyzna punkty w tym kryterium, jeżeli wykonawca wskaże czas reakcji na poziomie poniżej 120 minut.

Ocena ofert w ramach tego kryterium zostanie przeprowadzona na podstawie informacji wskazanych przez wykonawcę w Formularzu ofertowym.
W przypadku, gdy wykonawca w ofercie zaoferuje czas reakcji na zgłoszenie serwisowe na poziomie 120 minut, otrzyma w kryterium czas reakcji na zgłoszenie serwisowe (R) – 0,00 pkt.

W przypadku niewskazania przez Wykonawcę czasu reakcji na zgłoszenie serwisowe, Zamawiający przyjmie, iż oferowany przez Wykonawcę czas reakcji na zgłoszenie wynosi 120 minut, a w takim przypadku Wykonawca otrzyma 0 punktów w niniejszym kryterium.

W niniejszym kryterium nie dopuszcza się wskazania innego terminu niż wyrażonego w minutach. W przypadku, gdy wykonawca zaoferuje termin wyrażony inaczej niż wymaga zamawiający, jeśli będzie możliwe wyliczenie terminu, zamawiający przyjmie zaoferowaną pełną liczbę minut, w innym przypadku przyjmie, że wykonawca zaoferował maksymalny wymagany przez zamawiającego termin (tj. 120 minut), a wykonawca w niniejszym kryterium otrzyma 0 pkt.

c) najkrótszy czas podjęcia działań serwisowych od chwili reakcji na zgłoszenie serwisowe (T):

$$T = \frac{Tmin}{Ti} x100x20\%$$

gdzie: T – liczba punktów za najkrótszy czas podjęcia działań serwisowych
$T_{min}$-najkrótszy czas podjęcia działań serwisowych
$T_i$ – czas podjęcia działań serwisowych

Punkty w przedmiotowym kryterium zostaną przyznane jedynie temu wykonawcy, który w Formularzu ofertowym wskaże oferowany czas podjęcia działań serwisowych. Przy czym zamawiający przyzna punkty w tym kryterium, jeżeli wykonawca wskaże czas podjęcia działań serwisowych na poziomie poniżej 4 godzin.

Ocena ofert w ramach tego kryterium zostanie przeprowadzona na podstawie informacji wskazanych przez wykonawcę w Formularzu ofertowym.
W przypadku, gdy wykonawca w ofercie zaoferuje czas podjęcia działań serwisowych na poziomie 4 godzin, otrzyma w kryterium czas podjęcia działań serwisowych (T) – 0,00 pkt.

W przypadku niewskazania przez Wykonawcę czasu podjęcia działań serwisowych, Zamawiający przyjmie, iż oferowany przez Wykonawcę czas podjęcia działań serwisowych wynosi 4 godziny, a w takim przypadku Wykonawca otrzyma 0 punktów w niniejszym kryterium.

Zamawiający nie wyraża zgody na wskazanie terminu w tym kryterium, inaczej niż w godzinach. W przypadku, gdy wykonawca zaoferuje termin wyrażony inaczej niż wymaga Zamawiający, jeśli będzie możliwe wyliczenie terminu w godzinach, zamawiający przyjmie zaoferowaną pełną liczbę godzin, w innym przypadku przyjmie, że wykonawca zaoferował maksymalny wymagany przez zamawiającego termin, (tj. 4 godziny), a wykonawca w niniejszym kryterium otrzyma 0 pkt.

4) Ocenę ostateczną stanowić będzie łączna liczba punktów przyznanych wykonawcy za powyższe kryteria obliczona według wzoru:

$$C + R + T = P$$

gdzie:

C- liczba punktów za cenę ofertową,
R- liczba punktów za najkrótszy czas reakcji na zgłoszenie serwisowe,
T- liczba punktów za najkrótszy czas podjęcia działań serwisowych,
P - łączna liczba punktów przyznanych wykonawcy stanowiąca ostateczną ocenę badanej oferty.

**2. Wybór oferty najkorzystniejszej**

Zamawiający wybierze tę ofertę, która uzyska największą liczbę punktów łącznie we wszystkich kryteriach.

## ROZDZIAŁ IX. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

## ROZDZIAŁ X. FORMALNOŚCI, KTÓRE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY, W CELU ZAWARCIA UMOWY

1. Udział w przetargu jest jednoznaczny z przyjęciem warunków umowy zawartych w projekcie umowy stanowiącym Załącznik Nr 6 do specyfikacji istotnych warunków zamówienia.
2. Zamawiający zawrze umowę w sprawie zamówienia publicznego zgodnie z terminami i warunkami określonymi w art. 94 ustawy.
3. Zamawiający, przewiduje możliwość istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, w zakresie:
   1) terminu realizacji przedmiotu umowy w przypadku:
      a) wystąpienia okoliczności niezależnych od wykonawcy, przy zachowaniu przez niego należytej staranności, skutkujących niemożnością dotrzymania terminu realizacji przedmiotu umowy,
      b) wstrzymania przez zamawiającego wykonania prac niewynikających z okoliczności leżących po stronie wykonawcy (nie dotyczy okoliczności wstrzymania wykonywania dostawy w przypadku stwierdzenia nieprawidłowości zawinionych przez wykonawcę),
      c) wystąpienia siły wyższej, czyli zdarzenia zewnętrznego, którego skutków nie da się przewidzieć,
4. W przypadku zmian terminu realizacji przedmiotu umowy, wymienionych w ust. 3 pkt 1, termin ten może ulec przedłużeniu, jednak nie dłużej, niż o czas trwania tych okoliczności.
5. Postanowienia wymienione w ust. 3 stanowią katalog zmian, na które zamawiający może wyrazić zgodę, lecz nie stanowią one zobowiązania zamawiającego na ich wprowadzenie.
6. Zamawiający ma prawo rozwiązania umowy, w następujących przypadkach:
   1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach,
   2) nieotrzymania środków budżetowych koniecznych do realizacji niniejszej umowy od dysponenta odpowiedniego stopnia, w terminie 30 dni od dnia uzyskania informacji o powyższej okoliczności,
7. W sytuacji opisanej w ust. 6 pkt 1 i 2 umowa ulegnie rozwiązaniu, a wykonawcy przysługiwało będzie jedynie wynagrodzenie za zrealizowaną część umowy. Przepisów dotyczących kar umownych nie stosuje się.

8. Zamawiający przewiduje możliwość istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, w zakresie wysokości wynagrodzenia w przypadku zmiany:
   a) stawki podatku od towarów i usług,
   b) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (tekst jednolity: Dz. U. z 2017 r., poz. 847 ze zm.),
   c) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,

   - jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia publicznego przez wykonawcę, każda ze stron umowy może zwrócić się do drugiej strony, w terminie 30 dni od dnia wejścia w życie przepisów dokonujących powyższych zmian, z wnioskiem o dokonanie odpowiedniej zmiany wynagrodzenia.
9. Zmiana wysokości wynagrodzenia, na podstawie ust. 8 obowiązywać będzie od dnia wejścia w życie zmian, o których mowa odpowiednia w ust. 8 lit. a-c. Wykonawca najpóźniej w terminie 30 dni od wejścia w życie powyższych zmian, złoży oświadczenie , o którym mowa w ust.13.
10. W wypadku zmiany, o której mowa w ust. 8 lit. a, wartość netto wynagrodzenia wykonawcy nie zmieni się, a wartość brutto wynagrodzenia zostanie wyliczona z uwzględnieniem aktualnej stawki podatku VAT. W przypadku zmiany, o której mowa w ust. 8 lit. a stosowny aneks zostanie zawarty w terminie miesiąca od złożenia przez Wykonawcę wniosku wraz z ww. oświadczeniem.
11. W przypadku zmiany, o której mowa w ust. 8 lit. b, wynagrodzenie wykonawcy ulegnie zmianie adekwatnie o wartość wzrostu całkowitego kosztu wykonawcy wynikającą ze zwiększenia wynagrodzeń osób bezpośrednio wykonujących zamówienie do wysokości aktualnie obowiązującego minimalnego wynagrodzenia, z uwzględnieniem wszystkich obciążeń publicznoprawnych od kwoty wzrostu minimalnego wynagrodzenia.
12. W przypadku zmiany, o której mowa w ust. 8 lit. c, wynagrodzenie wykonawcy ulegnie zmianie adekwatnie o wartość wzrostu całkowitego kosztu wykonawcy, jaką będzie on zobowiązany dodatkowo ponieść w celu uwzględnienia tej zmiany, przy zachowaniu dotychczasowej kwoty netto wynagrodzenia osób bezpośrednio wykonujących zamówienie na rzecz zamawiającego.
13. Wprowadzenie zmiany wysokości wynagrodzenia, o której mowa w ust. 8 wymaga uprzedniego złożenia przez wykonawcę oświadczenia o wysokości dodatkowych kosztów wynikających z wprowadzenia zmian wraz z wykazaniem ich wysokości. W przypadku zmiany, o której mowa w ust. 8 lit. b-c, wykonawca zobowiązany jest do wykazania w jaki sposób ww. zmiany wpłynęły na wysokość wynagrodzenia wykonawcy, w szczególności do złożenia wykazu pracowników zatrudnionych na podstawie płacy minimalnej, kalkulacji kosztów pracy ww. pracowników wraz z podaniem obecnego wynagrodzenia oraz wynagrodzenia przed zmianą. Zamawiający zastrzega sobie prawo do żądania przedstawienia przez wykonawcę dokumentów potwierdzających zasadność złożenia takiego oświadczenia oraz wzrost kosztów
14. Wykonawca zobowiązuje się powiadomić zamawiającego o każdej zmianie danych i stanu faktycznego mających wpływ na realizację umowy.

## ROZDZIAŁ XI. ŚRODKI OCHRONY PRAWNEJ

Wykonawcom oraz innym osobom przewidzianym ustawą, których interes w uzyskaniu zamówienia doznał lub może doznać uszczerbku w wyniku naruszenia przez zamawiającego przepisów ustawy, przysługują środki ochrony prawnej przewidziane w Dziale VI ustawy do postępowań o wartości poniżej progu określonego na podstawie art. 11 ust. 8 ustawy.

**Załączniki do SIWZ:**

Załącznik Nr 1 – Szczegółowy opis przedmiotu zamówienia;
Załącznik Nr 2 – Formularz - Oferta przetargowa;
Załącznik Nr 3 – Formularz - Szczegółowy opis produktu;
Załącznik Nr 4 – Formularz - Oświadczenie o braku podstaw do wykluczenia z postępowania;
Załącznik Nr 5 – Formularz - Oświadczenie o przynależności do grupy kapitałowej;
Załącznik Nr 6 – Projekt umowy.

## Szczegółowy opis przedmiotu zamówienia

**Przedmiot zamówienia:** usługa zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego.
**Termin wykonania umowy:**
**I etap –** 30 dni od dnia podpisania umowy,
**II etap -** 36 miesięcy od dnia zakończenia I etapu
Wykonawca zapewni usługę zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach Zamawiającego przy:
- al. „Solidarności" 127 w Warszawie,
- ul. Czerniakowskiej 100 w Warszawie,
- ul. Płockiej 9 w Warszawie.

Wykonawca w terminie 30 dni od dnia podpisania umowy zobowiązuje się do udostepnienia urządzeń, dokonania ich konfiguracji oraz przeprowadzenia szkoleń.

Realizacja przedmiotu zamówienia wyodrębnia II etapy świadczenia usługi:

1) I etap:
   Wykonawca zapewni usługę zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach Zamawiającego przy:
   - al. „Solidarności" 127 w Warszawie,
   - ul. Czerniakowskiej 100 w Warszawie,
   - ul. Płockiej 9 w Warszawie.

   Usługa zabezpieczenia ściany ogniowej UTM będzie spełniała wymagania określone Szczegółowym opisie przedmiotu zamówienia, stanowiącym Załącznik Nr 1 do umowy. Wykonawca w ramach realizacji I etapu:
   a) zapewni świadczenie usługi zabezpieczenia ściany ogniowej UTM w lokalizacjach Sądu, przy użyciu zastosowanych urządzeń, będących własnością Wykonawcy, a kompatybilnych z urządzeniami FortiGate 51-E Hardware użytkowanymi przez Zamawiającego.
   b) dokona zakupu subskrypcji dla wszystkich zastosowanych urządzeń.
   c) przeprowadzi szkolenie dla administratorów sieci (do 5 osób) z zasad monitoringu dostarczonych urządzeń oraz zastosowanej konfiguracji.
2) II etap:
   Wykonawca zapewni wsparcie techniczne przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM. Wykonawca, w ramach wsparcia technicznego, obejmującego również połączenia zdalne VPN, zobowiązuje się do:
   a) podjęcia działań serwisowych zastosowanych urządzeń, najpóźniej w ciągu maksymalnie 4 godzin od zgłoszenia przez Zamawiającego, przy maksymalnie 120 minutowym czasie reakcji na zgłoszenie serwisowe, przy czym działania naprawcze będą podejmowane w godzinach 8:00 - 16:00 od poniedziałku do piątku,
   b) prowadzenia monitoringu zastosowanych urządzeń oraz w przypadku braku odpowiedzi na zapytania ICMP Echo Request ze strony urządzenia reagowania do następnego dnia roboczego,
   c) uaktualnienia ustawień sprzętowych urządzeń wskazanych w szczegółowym przedmiocie zamówienia w lokalizacjach wskazanych w pkt 1;
   d) rozwiązywania bieżących problemów występujących podczas pracy z systemem,
   e) pomocy w przypadku ewentualnych ataków sieciowych,
   f) analizy logów systemu,
   g) pomocy w opracowaniu metodologii wdrażania nowych funkcjonalności urządzenia,
   h) pośrednictwa w kontaktach z producentem urządzenia,

i) przyjmowania zgłoszeń serwisowych telefonicznie, za pośrednictwem poczty elektronicznej oraz dedykowanego portalu wsparcia technicznego,
j) okresowych wizyt „prewencyjnych" co dwa miesiące, realizowanych w czasie dogodnym dla Zamawiającego (wcześniej uzgodnionym z Zamawiającym),
k) zapewnienia dostępu do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc.,
l) przekazywania biuletynu informacyjnego dostarczanego drogą elektroniczną,
m) wykonywania uaktualnień ustawień sprzętowych urządzeń,
n) w przypadku awarii urządzeń ich wymiany na urządzenia o parametrach nie gorszych niż wymieniane,
o) pozostałe warunki dotyczące wsparcia są ujęte w szczegółowym opisie przedmiotu zamówienia.

## I. Świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego w lokalizacji przy al. „Solidarności" 127 w Warszawie:

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Usługa bezpieczeństwa musi zostać zbudowana w oparciu o urządzenia nowe zakupione w polskiej dystrybucji i wyprodukowane nie wcześniej niż 6 miesięcy przed datą realizacji usługi. Jako potwierdzenie ww. wymagania Wykonawca dostarczy oświadczenie producenta w tym zakresie.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
5. Dostarczony system powinien składać się z co najmniej dwóch urządzeń pracujących w klastrze Active-Pasive lub Active-Active.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.
5. System musi być wyposażony w redundantne zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 300 000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 22 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5.2 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4.7 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 5.7 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego SSH.

**Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dlaprotokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.

- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.

· Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 200 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxyavoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

**Logowanie**

1. System musi mieć możliwość logowania do zamawianego przez zamawiającego systemu logowania i raportowania.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPSec VPN.
- ICSA dla funkcji SSL VPN.

**Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

**Opisy do wymagań ogólnych**

1) W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2) Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

## II. Świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego w lokalizacjach przy ul. Płockiej 9 w Warszawie i ul. Czerniakowskiej 100 w Warszawie:

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z

odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Usługa bezpieczeństwa musi zostać zbudowana w oparciu o urządzenia nowe zakupione w polskiej dystrybucji i wyprodukowane nie wcześniej niż 6 miesięcy przed datą realizacji usługi. Jako potwierdzenie ww. wymagania Wykonawca dostarczy oświadczenie producenta w tym zakresie.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
5. Dostarczony system powinien składać się z co najmniej dwóch urządzeń pracujących w klastrze Active-Pasive lub Active-Active.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 18 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.
5. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 130 000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 9 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu HTTP - minimum 6 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 1 Gbps.

**Funkcje Systemu Bezpieczeństwa:**
W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego SSH.

**Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dlaprotokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.

- Policy Based Routingu.

· Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 200 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxyavoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

**Logowanie**

1. System musi mieć możliwość logowania do zamawianego przez zamawiającego systemu logowania i raportowania.
2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPSec VPN.
- ICSA dla funkcji SSL VPN.

**Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego

serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

**Opisy do wymagań ogólnych**

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**III. Świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego oraz centralizacji procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń Sądu Okręgowego w Warszawie – w lokalizacji przy al. „Solidarności" 127 w Warszawie:**

**Wymagania Ogólne**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Usługa bezpieczeństwa musi zostać zbudowana w oparciu o urządzenia nowe zakupione w polskiej dystrybucji i wyprodukowane nie wcześniej niż 6 miesięcy przed datą realizacji usługi. Jako potwierdzenie ww. wymagania Wykonawca dostarczy oświadczenie producenta w tym zakresie.

**Interfejsy, Dysk, Zasilanie:**

1. System musi dysponować co najmniej:
   - 4 portami Gigabit Ethernet RJ-45.
2. Rozwiązanie musi dysponować powierzchnią dyskową użytkową po zastosowaniu RAID 10 min. 5 TB.
3. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 10.

**Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 200 GB logów na dzień.
2. System musi być w stanie przeanalizować minimum 6000 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 200 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

**Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.

3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.
b. Listę najbardziej aktywnych użytkowników.
c. Listę najczęściej wykorzystywanych aplikacji.
d. Listę najczęściej odwiedzanych stron www.
e. Listę krajów , do których nawiązywane są połączenia.
f. Listę najczęściej wykorzystywanych polityk Firewall.
g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

**Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

**Opisy do wymagań ogólnych**

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Zamawiający na podstawie art. 29 ust. 3a nie wymaga zatrudnienia przez wykonawcę lub podwykonawcę na podstawie umowy o pracę osób wykonujących wskazane przez Zamawiającego czynności w zakresie realizacji niniejszego zamówienia, gdyż wykonanie tych czynności nie polega na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz. U. z 2018 r. poz. 108).

**Oferta przetargowa dla Zamawiającego:**
**Sąd Okręgowy w Warszawie**
**al. „Solidarności" 127,00-898 Warszawa**

Niżej podpisani .....

działając w imieniu i na rzecz .....

.....
*(nazwa i siedziba Wykonawcy)*

działającego w oparciu o wpis do ……..……, pod nr ……..

REGON:....., NIP:.....

tel. ..... fax. …….....

strona internetowa ..... e-mail .....

przystępując do uczestnictwa w postępowaniu o udzielenie zamówienia publicznego nr **ZP/OI/27/18** w trybie przetargu nieograniczonego, w oparciu o przepisy ustawy *z* dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r. poz. 1579 ze zm.), **na świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego**, składamy niniejszą ofertę:

1. Oferujemy wykonanie całego przedmiotu zamówienia za cenę:

   z podatkiem VAT: ..... zł,

   (słownie: .....),

   bez podatku VAT: ..... zł,

   (słownie: .....),

   w tym należny podatek VAT ……..%, w oparciu o cenę za:

   1) zapewnienie usługi zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach Zamawiającego przy:
      - al. „Solidarności" 127 w Warszawie,
      - ul. Czerniakowskiej 100 w Warszawie,
      - ul. Płockiej 9 w Warszawie,

      w okresie 30 dni od podpisania umowy:
      z podatkiem VAT: ……. zł
      (słownie: …….),
      stanowiące 70% całkowitego wynagrodzenia z podatkiem VAT, o którym mowa w ust. 1.*
   2) zapewnienie wsparcia technicznego przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM (36 miesięcy od zakończenia etapu I):
      z podatkiem VAT: ……. zł
      (słownie: …….),
      stanowiące 30% całkowitego wynagrodzenia z podatkiem VAT, o którym mowa w ust. 1.*
      w oparciu o cenę miesięcznego wynagrodzenia za świadczenie usługi w wysokości:
      z podatkiem VAT: ……zł
      (słownie:…….).

      **Określenie wartości poszczególnych etapów na innym poziomie niż 70% i 30% traktowane będzie jako błąd w obliczaniu ceny.*

2. Oświadczamy, iż przedmiot zamówienia zrealizujemy w terminie:
   1) I etap – zapewnienie usługi zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy- 30 dni od dnia podpisania umowy,
   2) II etap - zapewnienie wsparcia technicznego przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM- 36 miesięcy od dnia zakończenia I etapu.
3. Oświadczamy, że podane ceny zawierają wszelkie koszty niezbędne do zrealizowania przedmiotu zamówienia wynikające wprost ze Szczegółowego opisu przedmiotu zamówienia, stanowiącego Załącznik Nr 1 do specyfikacji istotnych warunków zamówienia, jak również w nim nie ujęte, a bez których nie można wykonać przedmiotu zamówienia oraz opisane w projekcie umowy, stanowiącym Załącznik Nr 6 do specyfikacji istotnych warunków zamówienia.
4. Oświadczamy, że czas podjęcia reakcji na zgłoszenia serwisowe wynosi …….. minut* (maksymalnie 120 minut).

   * *Przy czym zamawiający przyzna punkty w tym kryterium, jeżeli wykonawca wskaże czas reakcji na poziomie poniżej 120 minut.*
   *W przypadku, gdy Wykonawca w ofercie zaoferuje czas reakcji na zgłoszenie serwisowe na poziomie 120 minut, otrzyma w kryterium czas reakcji na zgłoszenie serwisowe (R) – 0,00 pkt.*
   *W przypadku niewskazania przez Wykonawcę czasu reakcji na zgłoszenie serwisowe, Zamawiający przyjmie, iż oferowany przez Wykonawcę czas reakcji na zgłoszenie wynosi 120 minut, a w takim przypadku Wykonawca otrzyma 0 punktów w niniejszym kryterium.*
   *W niniejszym kryterium nie dopuszcza się wskazania innego terminu niż wyrażonego w minutach. W przypadku, gdy Wykonawca zaoferuje termin wyrażony inaczej niż wymaga Zamawiający, jeśli będzie możliwe wyliczenie terminu, Zamawiający przyjmie zaoferowaną pełną liczbę minut, w innym przypadku przyjmie, że Wykonawca zaoferował maksymalny wymagany przez Zamawiającego termin (tj. 120 minut), a wykonawca w niniejszym kryterium otrzyma 0 pkt.*
5. Oświadczamy, że czas podjęcia działań serwisowych od chwili reakcji na zgłoszenie serwisowe wynosi ……. godzin**(maksymalnie 4 godziny).

   ** *Przy czym zamawiający przyzna punkty w tym kryterium, jeżeli wykonawca wskaże czas podjęcia działań serwisowych na poziomie poniżej 4 godzin*.
   *W przypadku, gdy Wykonawca w ofercie zaoferuje czas podjęcia działań serwisowych na poziomie 4 godzin, otrzyma w kryterium czas podjęcia działań serwisowych (T) – 0,00 pkt.*
   *W przypadku niewskazania przez Wykonawcę czasu podjęcia działań serwisowych, Zamawiający przyjmie, iż oferowany przez Wykonawcę czas podjęcia działań serwisowych wynosi 4 godziny, a w takim przypadku Wykonawca otrzyma 0 punktów w niniejszym kryterium.*
   *Zamawiający nie wyraża zgody na wskazanie terminu w tym kryterium, inaczej niż w godzinach. W przypadku, gdy wykonawca zaoferuje termin wyrażony inaczej niż wymaga Zamawiający, jeśli będzie możliwe wyliczenie terminu w godzinach, zamawiający przyjmie zaoferowaną pełną liczbę godzin, w innym przypadku przyjmie, że wykonawca zaoferował maksymalny wymagany przez zamawiającego.*
6. Oświadczamy, że przeprowadzimy szkolenia dla administratorów sieci w ilości do 5 osób z zasad monitoringu dostarczonych urządzeń oraz zastosowanej konfiguracji.
7. Oświadczamy, że oferowane przez nas usługi stanowiące przedmiot zamówienia spełniają wymagania określone przez Zamawiającego w Szczegółowym opisie przedmiotu zamówienia.
8. Oświadczamy, że do realizacji usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego użyjemy następujących urządzeń:
   1) ……
   2) ……
   3) ……
   4) ……
   5) ……,

   które są kompatybilne z urządzeniami posiadanymi przez Zamawiającego, wskazanymi w Szczegółowym opisie przedmiotu zamówienia.
9. W ramach przedmiotowej usługi dostarczymy wszelkie niezbędne licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmujące: kontrolę aplikacji, IPS, antywirus, antyspam, Web Filtering na okres …… (min. 36 miesiące)***.
10. Oświadczamy, iż oferowany system jest objęty gwarancją producenta na okres …… (min. 36miesięcy)*** odpowiednio od dnia świadczenia usługi, polegającą na naprawie lub wymianie w przypadku jego wadliwości. W ramach tego serwisu producent zapewni dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

    ****W przypadku niewskazania okresu w ust. 9 i 10 niniejszego formularza, Zamawiający przyjmie, że Wykonawca oferuje minimalny wymagany okres 36 miesięcy*
11. Oświadczamy, że akceptujemy postanowienia zawarte w „Projekcie umowy", stanowiącym Załącznik Nr 6 do specyfikacji istotnych warunków zamówienia i w przypadku wyboru naszej oferty zobowiązujemy się do zawarcia umowy na warunkach przedstawionych w projekcie umowy, w miejscu i terminie określonym przez Zamawiającego.
12. Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w specyfikacji istotnych warunków zamówienia, tj. 30 dni liczonych od upływu terminu składania ofert określonego w

specyfikacji istotnych warunków zamówienia.

13. Oświadczamy, że jeżeli w okresie związania ofertą nastąpią jakiekolwiek znaczące zmiany sytuacji przedstawionej w naszych dokumentach załączonych do oferty, natychmiast poinformujemy o nich Zamawiającego.
14. Osobami upoważnionymi do kontaktu z Zamawiającym oraz w przypadku wyboru oferty do nadzorowania wykonania umowy są:
    Pan/Pani: ....., tel./fax: .....
15. Oświadczamy, że wykonanie części zamówienia powierzymy **Podwykonawcom** *(należy podać nazwy (firm) Podwykonawców)*.

    1) ……

    2) ……

    3) ……

    w następującym zakresie:

    1) ……

    2) ……

    3) ……
16. Oświadczamy, zgodnie z art. 91 ust. 3a ustawy, że wybór naszej oferty:
    - ☐ nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług***
    - ☐ będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, zgodnie z przepisami o podatku od towarów i usług, w zakresie następujących towarów i usług***:

    nazwa: ……wartość:…….

    nazwa:……wartość:……

    nazwa: ……wartość:…….

    *(należy podać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, oraz wskazać ich wartość bez kwoty podatku)*
    ****właściwe zaznaczyć*
17. Oświadczam, iż jestem:
    - ☐ mikroprzedsiębiorcą****
    - ☐ małym przedsiębiorcą****
    - ☐ średnim przedsiębiorcą****
    - ☐ dużym przedsiębiorcą****

    **** *właściwe zaznaczyć*
18. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub 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. Urz. UE L 119 z 04.05.2016 r., str. 1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. *****

    *****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 (należy usunąć treści oświadczenia np. przez jego wykreślenie).
19. Numer rachunku bankowego Wykonawcy do rozliczeń z Zamawiającym:

    ……

20. Załącznikami do niniejszej oferty są:

1) .....

2) .....

3) .....

Oferta wraz z załącznikami zawiera ..... zapisanych stron, podpisanych i ponumerowanych zgodnie z wymogami specyfikacji istotnych warunków zamówienia.

..... dnia .....
*(miejscowość, data)*

……..…….....
*(podpis Wykonawcy lub osoby upoważnionej)*

# O Ś W I A D C Z E N I E
## O BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA
zgodnie z art. 25a ust. 1ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
(tekst jednolity: Dz. U. z 2017 r. poz. 1579 ze zm.).
(składane wraz z ofertą)

Przystępując do udziału w postępowaniu o zamówienie publiczne nr **ZP/OI/27/18 na świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego,** w imieniu reprezentowanego przeze mnie Wykonawcy (firmy/konsorcjum):

.....

.....
*(pełna nazwa i siedziba Wykonawcy, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

1) oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 12-23 ustawy,
2) oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …….. ustawy
*(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 ustawy Pzp).*
Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:……..
……..……..…
……
……
3) oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: ……..……
……
……
……
*(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*
nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.
**Punkt 3 niniejszego oświadczenia wypełniają Wykonawcy, którzy polegają na zasobach innych podmiotów.*

4) oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

..... dnia ……..……
*(miejscowość)*

.....
*(podpis Wykonawcy lub osoby upoważnionej)*

# O Ś W I A D C Z E N I E
# O P R Z Y N A L E Ż N O Ś C I DO G R U P Y K A P I T A Ł O W E J

**UWAGA!** OŚWIADCZENIE WYKONAWCA ZOBOWIĄZANY JEST ZŁOŻYĆ W TERMINIE 3 DNI OD DNIA ZAMIESZCZENIA NA STRONIE INTERNETOWEJ ZAMAWIAJĄCEGO INFORMACJI Z OTWARCIA OFERT, O KTÓREJ MOWA W ART. 86 USTAWY PZP

Przystępując do udziału w postępowaniu o zamówienie publiczne nr **ZP/OI/27/18 na świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego** w imieniu reprezentowanego przeze mnie Wykonawcy (firmy):

.....

.....
*((pełna nazwa i siedziba Wykonawcy, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

☐ oświadczamy, iż nie należymy do żadnej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2018 r., poz. 798 ze zm.)*****;

☐ oświadczamy, iż nie należymy do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2018 r., poz. 798 ze zm.), do której należą wykonawcy, którzy złożyli odrębne oferty ww. postępowaniu*****;

☐ oświadczamy, iż należymy do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz. U. z 2018 r., poz. 798 ze zm.), do której należy również wykonawca, który złożył odrębną ofertę ww. postępowaniu, tj.*:

……..…..
……..…….
……

***właściwe zaznaczyć**

....., dnia ..... r. .....
(miejscowość)*(podpis Wykonawcy lub osoby upoważnionej)*

**U M O W A Nr .....**
**(projekt)**

W dniu ……. w Warszawie, pomiędzy:

Skarbem Państwa - Sądem Okręgowym w Warszawie z siedzibą w Warszawie (00–898) przy al. Solidarności 127, NIP: 527-20-26-252, Regon: 000324694, zwanym w dalszej treści umowy „Zamawiającym", reprezentowanym przez:

……..

a

firmą ..... z siedzibą w …… przy ul. ……., NIP:……., Regon:……, działającą w oparciu o wpis do rejestru przedsiębiorców prowadzonego przez ……, pod numerem…….., posiadającą kapitał zakładowy w wysokości …….., zwaną w dalszej treści umowy „Wykonawcą", reprezentowaną przez:

.....,

zwanymi też w dalszej treści umowy „Stronami",

w wyniku udzielenia zamówienia publicznego nr **ZP/OI/27/18 na świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego**, w trybie przetargu nieograniczonego, na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r., poz. 1579ze zm.), zwanej dalej ustawą, została zawarta umowa o następującej treści:

**§ 1**
**Przedmiot umowy**

1. Przedmiotem umowy jest świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego dla Sądu Okręgowego w Warszawie za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach Zamawiającego:
   - al. „Solidarności" 127 w Warszawie,
   - ul. Czerniakowskiej 100 w Warszawie,
   - ul. Płockiej 9 w Warszawie,

   zgodnie z zapisami szczegółowego opisu przedmiotu zamówienia, stanowiącego Załącznik Nr 1 do umowy.
2. Wykonawca zobowiązuje się zrealizować przedmiot umowy zgodnie z jej treścią, wymaganiami określonymi w specyfikacji istotnych warunków zamówienia w postępowaniu o udzielenie zamówienia nr ZP/OI/27/18 oraz zobowiązaniami zawartymi w Ofercie Wykonawcy z dnia ……..2018 r., stanowiącej Załącznik Nr 2 do umowy.
3. Zamawiający zobowiązuje się współdziałać z Wykonawcą w zakresie umożliwiającym terminowe wywiązywanie się przez Wykonawcę z zobowiązań określonych w niniejszej umowie. Zamawiający zobowiązuje się do niezwłocznego udzielania Wykonawcy informacji niezbędnych do wykonania przedmiotu umowy.

**§ 2**
**Termin i zasady realizacji umowy**

1. Realizacja przedmiotu zamówienia wyodrębnia II etapy świadczenia usługi:
   1) I etap:
      Wykonawca zapewni usługę zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach Zamawiającego przy:
      - al. „Solidarności" 127 w Warszawie,
      - ul. Czerniakowskiej 100 w Warszawie,
      - ul. Płockiej 9 w Warszawie.

      Usługa zabezpieczenia ściany ogniowej UTM będzie spełniała wymagania określone Szczegółowym opisie przedmiotu zamówienia, stanowiącym Załącznik Nr 1 do umowy. Wykonawca w ramach realizacji I etapu:
      a) zapewni świadczenie usługi zabezpieczenia ściany ogniowej UTM w lokalizacjach Sądu, przy użyciu urządzeń ……., będących własnością Wykonawcy, a kompatybilnych z urządzeniami FortiGate 51-E Hardware użytkowanymi przez Zamawiającego.
      b) dokona zakupu subskrypcji dla wszystkich urządzeń……
      c) przeprowadzi szkolenie dla administratorów sieci (do 5 osób) z zasad monitoringu dostarczonych urządzeń oraz zastosowanej konfiguracji.
   2) II etap:
      Wykonawca zapewni wsparcie techniczne przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM. Wykonawca, w ramach wsparcia technicznego, obejmującego również połączenia zdalne VPN, zobowiązuje się do:
      a) podjęcia działań serwisowych urządzeń ……., najpóźniej w ciągu ……. godzin (max. 4 godziny) od zgłoszenia przez Zamawiającego, przy ……. (max. 120minut) czasie reakcji na zgłoszenie serwisowe, przy czym działania naprawcze będą podejmowane w godzinach 8:00 - 16:00 od poniedziałku do piątku,
      b) prowadzenia monitoringu urządzeń …… oraz w przypadku braku odpowiedzi na zapytania ICMP Echo Request ze strony urządzenia reagowania do następnego dnia roboczego,
      c) uaktualnienia ustawień sprzętowych urządzeń wskazanych w szczegółowym przedmiocie zamówienia w lokalizacjach wskazanych w pkt 1 umowy;
      d) rozwiązywania bieżących problemów występujących podczas pracy z systemem,
      e) pomocy w przypadku ewentualnych ataków sieciowych,
      f) analizy logów systemu,
      g) pomocy w opracowaniu metodologii wdrażania nowych funkcjonalności urządzenia,
      h) pośrednictwa w kontaktach z producentem urządzenia,
      i) przyjmowania zgłoszeń serwisowych telefonicznie, za pośrednictwem poczty elektronicznej oraz dedykowanego portalu wsparcia technicznego,
      j) okresowych wizyt „prewencyjnych" co dwa miesiące, realizowanych w czasie dogodnym dla Zamawiającego (wcześniej uzgodnionym z Zamawiającym),
      k) zapewnienia dostępu do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc.,
      l) przekazywania biuletynu informacyjnego dostarczanego drogą elektroniczną,
      m) wykonywania uaktualnień ustawień sprzętowych urządzeń,
      n) w przypadku awarii urządzeń ich wymiany na urządzenia o parametrach nie gorszych niż wymieniane,
      o) pozostałe warunki dotyczące wsparcia są ujęte w szczegółowym opisie przedmiotu zamówienia.
2. Termin realizacji umowy:
   1) I etap – zapewnienie usługi zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy- 30 dni od dnia podpisania umowy,
   2) II etap - zapewnienie wsparcia technicznego przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM - 36 miesięcy od dnia zakończenia I etapu.

3. Wszystkie czynności wykonywane w ramach zapewnienia usługi zabezpieczenia ściany ogniowej UTM będą każdorazowo dokumentowane w „Protokole realizacji usługi – etap I", którego wzór stanowi Załącznik Nr 3 do umowy.
   Niewykonanie przez Wykonawcę którejkolwiek z czynności stanowić będzie podstawę do naliczenia Wykonawcy kar umownych, zgodnie z § 7 ust. 1 pkt 3 umowy.
4. Wszystkie czynności wykonywane w ramach wsparcia technicznego będą każdorazowo dokumentowane w „Protokole realizacji usługi – etap II", którego wzór stanowi Załącznik Nr 4 do umowy.
   Niewykonanie przez Wykonawcę którejkolwiek z czynności stanowić będzie podstawę do naliczenia Wykonawcy kar umownych, § 7 ust. 1 pkt 4 umowy.
5. Do realizacji usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego użyjemy następujących urządzeń:
   1) ……..……
   2) ……..…….
   3) ……..…….
   4) ……..…….
   5) ……..……,
   które są kompatybilne z urządzeniami posiadanymi przez Zamawiającego, wskazanymi w Szczegółowym opisie przedmiotu zamówienia.
6. W okresie obowiązywania umowy usługa administrowana będzie wyłącznie przez Zamawiającego. Wykonawca nie ponosi odpowiedzialności za działania osób, które uzyskały dostęp do systemu w sposób nieuprawniony, z wyjątkiem pracowników Wykonawcy lub innych osób działających na jego zlecenie.
7. Wykonawca jest odpowiedzialny za działania lub zaniechania wszelkich osób, z pomocą których wykonuje niniejszą umowę, jak za własne działania lub zaniechania.
8. Wykonawca zobowiązuje się do dokonania czynności, do których zobowiązany jest na mocy niniejszej umowy, z należytą starannością. Wykonawca nie ponosi odpowiedzialności za wady urządzeń, ich oprogramowania oraz niewłaściwe działanie systemu, jeżeli nie powstały one z przyczyn leżących po stronie Wykonawcy w związku z wykonaniem niniejszej umowy.

**§ 3**
**Zobowiązania Zamawiającego**

Zamawiający w ramach realizacji niniejszej umowy zobowiązuje się do:
1) zapewnienia dostępu do Internetu w lokalizacjach objętym umową,
2) zapewnienia dostępu do pomieszczeń, w których znajdują się zarządzane urządzenia,
3) współpracy z należytą starannością z Wykonawcą.

**§ 4**
**Cena umowy i warunki płatności**

1. Całkowite wynagrodzenie Wykonawcy za przedmiot zamówienia (cena umowy) obejmujący świadczenie usługi zabezpieczenia ściany ogniowej UTM wraz z zapewnieniem wsparcia technicznego dla Sądu Okręgowego w Warszawie, nie przekroczy kwoty:
   z podatkiem VAT: ..... zł,
   (słownie: .....),
   bez podatku VAT: ..... zł,
   (słownie: .....),
   w tym należny podatek VAT ……..%,
   w oparciu o cenę:
   1) zapewnienie usługi zabezpieczenia ściany ogniowej UTM za pomocą 6 urządzeń firewall oraz jednego urządzenia do logowania i raportowania na okres obowiązywania umowy, które będą znajdowały się w budynkach Zamawiającego przy:
   - al. „Solidarności" 127 w Warszawie,
   - ul. Czerniakowskiej 100 w Warszawie,

- ul. Płockiej 9 w Warszawie,
z podatkiem VAT: ……zł
(słownie: ……),
stanowiące 70,% całkowitego wynagrodzenia z podatkiem VAT, o którym mowa w ust. 1.
2) zapewnienie wsparcia technicznego przez okres obowiązywania umowy w związku ze świadczeniem usługi zabezpieczenia ściany ogniowej UTM:
z podatkiem VAT: …….. zł
(słownie: ……),
stanowiące 30% całkowitego wynagrodzenia z podatkiem VAT, o którym mowa w ust. 1.
w oparciu o cenę miesięcznego wynagrodzenia za świadczenie usługi w wysokości:
z podatkiem VAT: ……zł
(słownie:……).

2. Cena, o której mowa w ust. 1, obejmuje wszystkie koszty niezbędne do zrealizowania zamówienia wynikające ze szczegółowego opisu przedmiotu zamówienia.
3. Cena umowy jest stała i nie ulegnie zmianie do końca trwania umowy.
4. Wynagrodzenie Wykonawcy, o którym mowa w ust. 1 pkt 1 przekazane zostanie poleceniem przelewu na rachunek bankowy Wykonawcy wskazany w ust. 10, w terminie do 30 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT.
5. Podstawą do wystawienia przez Wykonawcę faktury VAT za zrealizowanie I etapu przedmiotu umowy będzie podpisany, bez zastrzeżeń przez przedstawicieli obu Stron, powołanych w § 5 ust. 1 umowy, „Protokół realizacji usługi I etap", stanowiący Załącznik Nr 3 do umowy.
6. Miesięczne wynagrodzenie Wykonawcy, o którym mowa w ust. 1 pkt 2 przekazane zostanie poleceniem przelewu na rachunek bankowy Wykonawcy wskazany w ust. 10, raz w miesiącu po upływie pełnego miesiąca (nie kalendarzowego), w terminie do 30 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT.
7. Podstawą do wystawienia przez Wykonawcę faktury VAT za realizowanie II etapu przedmiotu umowy będzie każdorazowo podpisany, bez zastrzeżeń przez przedstawicieli obu Stron, powołanych w § 5 ust. 1 umowy, „Protokół realizacji usługi II etap", stanowiący Załącznik Nr 4 do umowy.
8. Za datę zapłaty uznaje się datę obciążenia rachunku bankowego Zamawiającego. Termin zapłaty uważa się za zachowany, jeżeli obciążenie rachunku bankowego Zamawiającego nastąpi najpóźniej w ostatnim dniu terminu płatności.
9. Faktury VAT wystawione będą na Sąd Okręgowy w Warszawie, płatnikiem będzie Sąd Okręgowy w Warszawie. Łączna wartość kwot z wystawionych faktur nie może przekroczyć kwoty wskazanej w ust. 1 umowy.
10. Numer rachunku bankowego Wykonawcy do rozliczeń z Zamawiającym:
……
Zmiana rachunku bankowego nie stanowi zmiany treści umowy i wymaga pisemnego poinformowana o powyższym Zamawiającego.
11. W razie opóźnienia płatności Wykonawca naliczyć może odsetki ustawowe za opóźnienie w zapłacie.

**§ 5**
**Nadzór prawidłowego wykonania przedmiotu umowy**

1. Osobami odpowiedzialnymi za nadzór nad prawidłowym wykonywaniem przedmiotu umowy są:
   1) po stronie Zamawiającego
   ……, tel. …….., e-mail: .....
   ……, tel. …….., e-mail: .....
   2) po stronie Wykonawcy:
   ……, tel. ……..……, e-mail:…….. .
2. Każda ze Stron umowy może dokonać zmiany osób, o których mowa w ust. 1, w drodze pisemnego oświadczenia złożonego drugiej Stronie, bez konieczności podpisywania aneksu.

**§ 6**
**Gwarancja jakości**

1. Oświadczamy, że oferowane przez nas usługi stanowiące przedmiot zamówienia spełniają wymagania określone przez Zamawiającego w Szczegółowym opisie przedmiotu zamówienia.
2. W ramach przedmiotowej usługi dostarczymy wszelkie niezbędne licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmujące: kontrolę aplikacji, IPS, antywirus, antyspam, Web Filtering na okres …… (min. 36 miesiące).
3. Oświadczamy, iż oferowany system jest objęty gwarancją producenta na okres …… (min. 36 miesięcy) odpowiednio od dnia świadczenia usługi, polegającą na naprawie lub wymianie w przypadku jego wadliwości. W ramach tego serwisu producent zapewni dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.
4. W przypadku awarii urządzenia i przerwy w świadczeniu usługi trwającej powyżej 3 godzin, od zgłoszenia dokonanego przez Zamawiającego, Wykonawca zobowiązany będzie zapewnić Zamawiającemu urządzenie zastępcze umożliwiające korzystanie przez Zamawiającego z przedmiotowej usługi w pełnym zakresie.

**§ 7**
**Odpowiedzialność odszkodowawcza i kary umowne**

1. Zamawiający może naliczyć kary umowne:
   1) w przypadku zwłoki w zakresie wykonania etapu I w terminie określonym w § 2 ust. 2 pkt 1 umowy, w wysokości 0,2 % wynagrodzenia, o którym mowa w § 4 ust. 1 pkt 1 umowy, za każdy dzień zwłoki
   2) w przypadku zwłoki w podjęciu działań serwisowych przy wskazanym czasie reakcji na zgłoszenie serwisowe w terminach określonych w § 2 ust. 1 pkt 2 lit. a-b umowy, w wysokości 0,2% całkowitego wynagrodzenia z podatkiem VAT, o którym mowa w § 4 ust. 1 pkt 2 umowy, odpowiednio za każdą rozpoczętą godzinę zwłoki – dla terminów liczonych w godzinach, za każde rozpoczęte pięć minut zwłoki – dla terminów liczonych w minutach, za każdy rozpoczęty dzień zwłoki - dla terminów liczonych w dniach,
   3) w przypadku nienależytego wykonania obowiązków przez Wykonawcę określonych w § 2 ust.1 pkt 1 lit. a-c umowy Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% całkowitego wynagrodzenia, o którym mowa w § 4 ust. 1 pkt 1 umowy za każdy przypadek,
   4) w przypadku nienależytego wykonania obowiązków przez Wykonawcę określonych w § 2 ust. 1 pkt 2 lit. c-o umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% całkowitego wynagrodzenia, o którym mowa w § 4 ust. 1 pkt 2 umowy za każdy przypadek,
   5) w przypadku niezapewnienia przez Wykonawcę urządzenia zastępczego, w terminie, o którym mowa w § 6 ust. 4 umowy, Zamawiający ma prawo do naliczania kary umownej w wysokości 10 % wynagrodzenia miesięcznego, o którym mowa w § 4 ust. 1 pkt 2 umowy, za każdą rozpoczętą godzinę zwłoki.
2. Zapłata kary umownej nie zwalnia Wykonawcy od podjęcia czynności zmierzających do prawidłowego wykonania usługi. W przypadku nie podjęcia tych czynności zamawiający zastrzega sobie prawo odstąpienia od umowy w terminie 30 dni od dnia powzięcia wiadomości o tej okoliczności.
3. Jeżeli zwłoka w terminach, o których mowa w ust. 1 pkt 3, przekroczy 8 godzin dla terminów liczonych w godzinach, 120 minut dla terminów liczonych w minutach, 5 dni roboczych dla terminów liczonych w dniach Zamawiający ma prawo odstąpić od zawartej umowy i naliczyć z tego tytułu karę umowną w wysokości 10 % całkowitej wartości umowy wskazanej w § 4 ust. 1 pkt 2 umowy.
4. W przypadku odstąpienia od umowy lub rozwiązania umowy przez którąkolwiek ze Stron, z przyczyn leżących po drugiej Stronie, ta ostatnia zapłaci karę umowną w wysokości 10% całkowitego wynagrodzenia Wykonawcy, określonego w § 4 ust. 1, w zależności od etapu, którego dotyczy.
5. W przypadku odstąpienia od umowy lub rozwiązania umowy przez którąkolwiek ze Stron, z przyczyn nieleżących po drugiej Stronie, ta ostatnia zapłaci karę umowną w wysokości 10%wynagrodzenia Wykonawcy, określonego w § 4 ust. 1, w zależności od etapu, którego dotyczy.
6. Przewidziane kary umowne nie wyłączają możliwości dochodzenia przez Strony odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych.

7. Wykonawca zobowiązuje się pokryć wszystkie szkody poniesione przez Zamawiającego lub osoby trzecie, powstałe w czasie wykonywania niniejszej umowy z przyczyn leżących po stronie Wykonawcy, wynikłe z wadliwego lub nieterminowego wykonania umowy.
8. Łączna wysokość kar umownych naliczonych przez Zamawiającego, w związku z realizacją niniejszej umowy, nie może przekroczyć wysokości 30% całkowitego wynagrodzenia, o którym mowa w § 4 ust. 1 umowy.
9. Wykonawca wyraża zgodę na potrącenie przez Zamawiającego kar umownych z przysługującej Wykonawcy należności, na podstawie noty księgowej wystawionej przez Zamawiającego.
10. W przypadku konieczności naliczenia Wykonawcy kar umownych, Zamawiający może wystawić Wykonawcy wezwanie do ich zapłaty, zaś Wykonawca zobowiązuje się do zapłaty naliczonych kar umownych, na rachunek wskazany w wezwaniu Zamawiającego, w terminie 7 dni od dnia doręczenia wezwania.

**§ 8**
**Odstąpienie i rozwiązanie umowy**

1. Każda ze Stron może rozwiązać umowę w trybie natychmiastowym z powodu niedotrzymania przez drugą Stronę istotnych warunków umowy w terminie 30 dni od dnia powzięcia wiadomości o tej okoliczności. Przepis § 7 ust. 5 umowy stosuje się odpowiednio.
2. Odstąpienie od umowy lub rozwiązanie umowy wymaga formy pisemnej pod rygorem nieważności.
3. Umowa może zostać rozwiązana w każdym czasie za zgodnym porozumieniem Stron bez zachowania okresów wypowiedzenia i naliczania kar umownych.
4. Zamawiający ma prawo rozwiązania umowy, w następujących przypadkach:
   1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach,
   2) nieotrzymania środków budżetowych koniecznych do realizacji niniejszej umowy od dysponenta odpowiedniego stopnia, w terminie 30 dni od dnia uzyskania informacji o powyższej okoliczności,
5. W przypadku opisanym w ust. 4 Wykonawcy przysługiwało będzie jedynie wynagrodzenie za zrealizowaną część umowy. Przepisy § 7 ust. 4umowy nie mają zastosowania.

**§ 9**
**Obowiązek informacyjny i bezpieczeństwo informacji**

1. Administratorem danych osobowych przedstawicieli Wykonawcy oraz wskazanych przez niego osób uczestniczących w wykonaniu zamówienia przetwarzanych w Sądzie Okręgowym w Warszawie jest Prezes Sądu Okręgowego w Warszawie z siedzibą w Warszawie, al. „Solidarności" 127;
2. Kontakt z inspektorem ochrony danych, który sprawuje nadzór nad ochroną danych osobowych w Sądzie Okręgowym w Warszawie realizowany jest za pośrednictwem adresu mailowego: iod@warszawa.so.gov.pl;
3. Administratorem danych osobowych przedstawicieli Zamawiającego przetwarzanych przez Wykonawcę jest ……
4. Dane osobowe, o których mowa w ust. 1 i 3 przetwarzane będą w celu związanym z postępowaniem o udzielenie zamówienia publicznego i realizacją niniejszej umowy oraz w celach księgowych;
5. Odbiorcami danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r. poz. 1579 ze zm.), dalej „ustawa Pzp";
6. Dane osobowe, o których mowa w ust. 1 będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy. Po upływie tego okresu – zgodnie z przepisami dotyczącymi archiwizacji dokumentacji;
7. Dane osobowe, o których mowa w ust. 3 będą przechowywane ……
8. Obowiązek podania przez Wykonawcę danych osobowych osób/y uprawnionych do reprezentowania Wykonawcy jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem

w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

9. Przedstawiciele Wykonawcy oraz osoby uczestniczące w realizacji zamówienia oraz przedstawiciele Zamawiającego mają prawo do: dostępu do swoich danych, ich sprostowania oraz ograniczenia ich przetwarzania a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają Państwo, że przetwarzanie danych osobowych narusza przepisy ochrony danych;
10. Realizacja praw, o których mowa w ust. 9 możliwa jest
    1) u Zamawiającego za pośrednictwem inspektora ochrony danych (iod@warszawa.so.gov.pl)
    2) u Wykonawcy ……..
11. Dane osobowe, o których mowa w ust. 1 i 3 nie będą przetwarzane w celach związanych z automatycznym podejmowanie decyzji w tym w oparciu o profilowanie;
12. Strony oświadczają, że dane osobowe udostępnione podczas i w związku z realizacją niniejszej umowy będą przetwarzane przez Strony zgodnie z przepisami 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 oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000) w celu realizacji niniejszej umowy;
13. Strony zobowiązują się do:
    1) wzajemnego stosowania zasad poufności dokumentów i informacji uzyskanych od drugiej Strony w związku z wykonywanym przedmiotem umowy zarówno w trakcie jej trwania jak i po ustaniu stosunku wynikającego z umowy;
    2) zabezpieczania przed kradzieżą, uszkodzeniem i zaginięciem wszelkich otrzymanych dokumentów (w tym na mobilnych nośnikach) związanych z przedmiotem umowy;
    3) niewykorzystywania zebranych informacji prawnie chronionych dla celów innych niż wynikające z realizacji umowy.
    4) niezwłocznego przekazywania drugiej Stronie informacji o wszelkich przypadkach naruszenia tajemnicy informacji prawnie chronionych lub o ich niewłaściwym użyciu.
14. Obowiązek zachowania poufności nie dotyczy informacji lub materiałów:
    1) których ujawnienie jest wymagane przez bezwzględnie obowiązujące przepisy prawa,
    2) których ujawnienie następuje na żądanie podmiotu uprawnionego do kontroli, pod warunkiem, że podmiot ten został poinformowany o poufnym charakterze informacji, które są powszechnie znane,
    3) które Strona uzyskała lub uzyska od osoby trzeciej, jeżeli przepisy obowiązującego prawa lub zobowiązanie umowne wiążące tę osobę nie zakazują ujawniania przez nią tych informacji i o ile Strona nie zobowiązała się do zachowania poufności,
    4) w których posiadanie Strona weszła zgodnie z obowiązującymi przepisami prawa, przed dniem uzyskania takich informacji na podstawie niniejszej umowy.
15. W wypadku, gdy jedna ze Stron zostanie zobowiązana nakazem sądu bądź organu administracji państwowej do ujawnienia informacji lub materiałów albo konieczność ich ujawnienia będzie wynikała z przepisów prawa, zobowiązuje się niezwłocznie pisemnie powiadomić o tym fakcie drugą Stronę.
16. Wykonawca zobowiązuje się do zapoznania osób odpowiedzialnych za realizację umowy z wyciągiem z Polityki Bezpieczeństwa Informacji wraz z klauzulą informacyjną dotyczącą przetwarzania danych osobowych stanowiącym Załącznik Nr 5 do umowy.

**§ 10**
**Postanowienia końcowe**

1. Wykonawca nie może przenosić wierzytelności wynikającej z umowy na rzecz osoby trzeciej, bez pisemnej zgody Zamawiającego.
2. Wykonawca nie może powierzyć realizacji umowy innemu Wykonawcy, bez pisemnej zgody Zamawiającego.
3. W razie naruszenia przez Wykonawcę postanowień zawartych w ust. 1 lub 2, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o którejkolwiek z tych okoliczności. Przepis § 7 ust. 4 umowy stosuje się odpowiednio.
4. Zamawiający, przewiduje możliwość istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, w zakresie:
    1) terminu realizacji przedmiotu umowy w przypadku:

a) wystąpienia okoliczności niezależnych od wykonawcy, przy zachowaniu przez niego należytej staranności, skutkujących niemożnością dotrzymania terminu realizacji przedmiotu umowy,
b) wstrzymania przez zamawiającego wykonania prac niewynikających z okoliczności leżących po stronie wykonawcy (nie dotyczy okoliczności wstrzymania wykonywania dostawy w przypadku stwierdzenia nieprawidłowości zawinionych przez wykonawcę),
c) wystąpienia siły wyższej, czyli zdarzenia zewnętrznego, którego skutków nie da się przewidzieć,

5. W przypadku zmian terminu realizacji przedmiotu umowy, wymienionych w ust. 4 pkt 1, termin ten może ulec przedłużeniu, jednak nie dłużej, niż o czas trwania tych okoliczności.
6. Postanowienia wymienione w ust. 4 stanowią katalog zmian, na które zamawiający może wyrazić zgodę, lecz nie stanowią one zobowiązania zamawiającego na ich wprowadzenie.
7. Zamawiający przewiduje możliwość istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, w zakresie wysokości wynagrodzenia w przypadku zmiany:
   1) stawki podatku od towarów i usług,
   2) wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (tekst jednolity: Dz. U. z 2017 r., poz. 847 ze zm.),
   3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne,

   - jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia publicznego przez wykonawcę, każda ze stron umowy może zwrócić się do drugiej strony, w terminie 30 dni od dnia wejścia w życie przepisów dokonujących powyższych zmian, z wnioskiem o dokonanie odpowiedniej zmiany wynagrodzenia.
8. Zmiana wysokości wynagrodzenia, dokonywana na podstawie ust. 7 obowiązywać będzie od dnia wejścia w życie zmian, o których mowa odpowiednio w ust. 7 lit. a-c. Wykonawca najpóźniej w terminie 30 dni od wejścia w życie zmian, o których mowa odpowiednio w ust. 7, złoży oświadczenie, o którym mowa w ust. 12.
9. W wypadku zmiany, o której mowa w ust. 7 lit. a, wartość netto wynagrodzenia wykonawcy nie zmieni się, a wartość brutto wynagrodzenia zostanie wyliczona z uwzględnieniem aktualnej stawki podatku VAT. W przypadku zmiany, o której mowa w ust. 7 lit. a stosowny aneks zostanie zawarty w terminie miesiąca od złożenia przez Wykonawcę wniosku wraz z ww. oświadczeniem.
10. W przypadku zmiany, o której mowa w ust. 7 lit. b, wynagrodzenie wykonawcy ulegnie zmianie adekwatnie o wartość wzrostu całkowitego kosztu wykonawcy wynikającą ze zwiększenia wynagrodzeń osób bezpośrednio wykonujących zamówienie do wysokości aktualnie obowiązującego minimalnego wynagrodzenia, z uwzględnieniem wszystkich obciążeń publicznoprawnych od kwoty wzrostu minimalnego wynagrodzenia.
11. W przypadku zmiany, o której mowa w ust. 7 lit. c, wynagrodzenie wykonawcy ulegnie zmianie adekwatnie o wartość wzrostu całkowitego kosztu wykonawcy, jaką będzie on zobowiązany dodatkowo ponieść w celu uwzględnienia tej zmiany, przy zachowaniu dotychczasowej kwoty netto wynagrodzenia osób bezpośrednio wykonujących zamówienie na rzecz zamawiającego.
12. Wprowadzenie zmiany wysokości wynagrodzenia, o której mowa w ust. 7 wymaga uprzedniego złożenia przez wykonawcę oświadczenia o wysokości dodatkowych kosztów wynikających z wprowadzenia zmian wraz z wykazaniem ich wysokości. W przypadku zmiany, o której mowa w ust. 7 lit. b-c, wykonawca zobowiązany jest do wykazania w jaki sposób ww. zmiany wpłynęły na wysokość wynagrodzenia wykonawcy, w szczególności do złożenia wykazu pracowników zatrudnionych na podstawie płacy minimalnej, kalkulacji kosztów pracy ww. pracowników wraz z podaniem obecnego wynagrodzenia oraz wynagrodzenia przed zmianą. Zamawiający zastrzega sobie prawo do żądania przedstawienia przez wykonawcę dokumentów potwierdzających zasadność złożenia takiego oświadczenia oraz wzrost kosztów.
13. Wykonawca zobowiązuje się powiadomić Zamawiającego o każdej zmianie danych i stanu faktycznego mających wpływ na realizację umowy.
14. Zmiana umowy może być dokonana wyłącznie w formie pisemnej pod rygorem nieważności.
15. Strony będą dążyły do polubownego rozstrzygania wszelkich sporów powstałych w związku z niniejszą umową, jednak w przypadku, gdy nie osiągną porozumienia, zaistniały spór będzie poddany rozstrzygnięciu przez sąd powszechny właściwy miejscowo dla Zamawiającego.

16. W sprawach nieuregulowanych niniejszą umową zastosowanie mają odpowiednie przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych z odnośnymi przepisami wykonawczymi.
17. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

**§ 11**
**Załączniki do umowy**

Integralną część niniejszej umowy stanowią niżej wymienione załączniki:
1) Załącznik Nr 1 – Szczegółowy opis przedmiotu zamówienia,
2) Załącznik Nr 2 – Oferta Wykonawcy z dnia ……..…….. r.,
3) Załącznik Nr 3 – „Protokół realizacji usługi – etap I”,
4) Załącznik Nr 4 – „Protokół realizacji usługi – etap II”,,
5) Załącznik Nr 5 – Wyciąg z polityk bezpieczeństwa Sądu Okręgowego w Warszawie.

**Z A M A W I A J Ą C Y** **W Y K O N A W C A**

Załącznik Nr 3do umowy

**PROTOKÓŁ REALIZACJI USŁUGI – etap I**

**Zamawiający**: Sąd Okręgowy w Warszawie, al. „Solidarności” 127, 00-898 Warszawa

**Wykonawca**: .....

Dnia .....

Niniejszym potwierdzam zapewnienie usługi zabezpieczenia ściany ogniowej UTM poprzez udostępnienie następujących urządzeń:

……

……

zgodnie z umową nr …….. z dnia ……. r.

Uwagi:
……

……

……

……

…….. ……. …….
(podpis przedstawiciela Wykonawcy) (podpis przedstawiciela Zamawiającego)

Załącznik Nr 4 do umowy

**PROTOKÓŁ REALIZACJI USŁUGI – etap II**

**Zamawiający**: Sąd Okręgowy w Warszawie, al. „Solidarności” 127, 00-898 Warszawa

**Wykonawca**: .....

Dnia .....

Niniejszym potwierdzam sprawowanie w okresie ……wsparcia technicznego przez Wykonawcę nad urządzeniami:

……

……

zgodnie z umową nr …….. z dnia ……. r.

Uwagi:
……

……

……

……

…….. ……. ……
(podpis przedstawiciela Wykonawcy) (podpis przedstawiciela Zamawiającego)

# WYCIĄG Z POLITYK BEZPIECZEŃSTWA SĄDU OKRĘGOWEGO W WARSZAWIE

## 1. Ogólne zasady bezpieczeństwa informacji

Wszyscy pracownicy Sądu oraz osoby wykonujące zadania na rzecz Sądu na podstawie umowy innej niż umowa o pracę są zapoznawani z regułami oraz z aktualnymi procedurami ochrony informacji oraz zobowiązani do ochrony informacji i przestrzegania zapisów PBI.
Poniższe uniwersalne zasady są podstawą realizacji PBI:

1. **Zasada uprawnionego dostępu**. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
2. **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
3. **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada usług koniecznych**. Udostępniane powinny być tylko takie usługi, jakie są konieczne do realizacji zadań.
5. **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). w przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.
6. **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.

7. **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
8. **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
9. **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
10. **Zasada najsłabszego ogniwa**. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
11. **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
12. **Zasada ewolucji**. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
13. **Zasada odpowiedniości**. Używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.
14. **Zasada świadomej konwersacji.** Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
15. **Zasada segregacji zadań.** Zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełni władzy nad całym systemem.

## 12. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

W Sądzie zarządza się zdarzeniami i incydentami związanymi z bezpieczeństwem informacji. Zarządzanie zdarzeniami i incydentami odbywa się w ramach procesu zarządzania incydentem.

Ogólne zasady zarządzania incydentem:

1. każdy zauważony incydent powinien zostać zgłoszony i zarejestrowany – musi nastąpić na niego reakcja;
2. wykryty incydent związany z naruszeniem bezpieczeństwa informacji chronionej należy bezzwłocznie zgłosić zgodnie z poniższym schematem:

Pracownik → Kierownik → ABI i ABS → Kierownictwo Sądu

podejmują adekwatne działania

3. w przypadku wystąpienia klęski żywiołowej lub aktu terroru w pierwszej kolejności powiadamiane są właściwe służby (Policja/Pogotowie Ratunkowe/Straż Pożarna), a następnie ochrona budynku oraz Prezes Sądu i Dyrektor Sądu – postępowanie w sytuacjach kryzysowych regulują odrębne procedury;
4. w przypadku zauważenia próby włamania, kradzieży dokumentów lub sprzętu oraz wszelkich innych prób niszczenia mienia powiadamiana jest ochrona budynku oraz bezpośredni przełożony lub osoba go zastępująca;
5. ochrona obiektu rejestruje incydenty we własnych dokumentach.

**Polityka Bezpieczeństwa Danych Osobowych**

1. przetwarzanie danych osobowych w systemach informatycznych jest dopuszczalne wyłącznie przez osobę posiadającą pisemne upoważnienie do przetwarzania danych osobowych;
2. dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora (loginu) i właściwego hasła;
3. identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, który ponosi odpowiedzialność za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji lub przekazania w celu naprawy podmiotowi nieuprawnionemu do przetwarzania danych osobowych pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

Użytkując komputer przenośny, zawierający dane osobowe, należy zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem wskazanym w wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Należy stosować środki ochrony kryptograficznej w stosunku do danych osobowych przetwarzanych na komputerach przenośnych, o ile są używane poza obszarem przetwarzania danych osobowych.

Kierownicy poszczególnych komórek organizacyjnych mają obowiązek zawiadomić ABS lub IOD o wszelkich incydentach zagrażających bezpieczeństwu danych osobowych przetwarzanych w systemach, wynikających z braku, niedoskonałości lub uszkodzeniu zabezpieczeń systemów teleinformatycznych.

**Upoważnienie do przetwarzania danych osobowych**

W tut. Sądzie przykłada się szczególną wagę do zapewnienia bezpieczeństwa wszystkim przetwarzanym danym osobowym oraz zapewnienia zgodności przyjętych norm z obowiązującymi przepisami prawa, dlatego przystąpienie do wykonywania powierzonych obowiązków przez nowozatrudnioną osobę w tut. Sądzie poprzedzone jest m.in. nadaniem przez ADO imiennego upoważnienia do przetwarzania danych osobowych w systemach teleinformatycznych oraz w tradycyjnych (papierowych) zbiorach danych temu pracownikowi oraz przyznaniem uprawnień do systemów teleinformatycznych – o ile ADO uwzględni w tym przedmiocie wniosek złożony przez Kierownika komórki organizacyjnej.

**Klauzula informacyjna dla osób wskazanych przez wykonawcę do realizacji zamówienia**

Administratorem Pani/Pana danych osobowych przetwarzanych w Sądzie Okręgowym w Warszawie jest Prezes Sądu Okręgowego w Warszawie z siedzibą w Warszawie, al. „Solidarności" 127.

1. Kontakt z inspektorem ochrony danych, który sprawuje nadzór nad ochroną danych osobowych w Sądzie Okręgowym w Warszawie realizowany jest za pośrednictwem adresu mailowego: iod@warszawa.so.gov.pl

2. Pani/Pana dane osobowe przetwarzane będą w celu związanym z postępowaniem o udzielenie zamówienia publicznego **ZP/OI/27/18** prowadzonym w trybie przetargu nieograniczonego i zostały Administratorowi udostępnione przez ……

3. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29

stycznia 2004 r. – Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r. poz. 1579 ze zm.), dalej „ustawa Pzp”;

4. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

5. Ma Pani/Pan prawo do: dostępu do swoich danych, ich sprostowania, usunięcia oraz ograniczenia ich przetwarzania a także prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ochrony danych;

6. Realizacja praw, o których mowa w pkt 5 możliwa jest za pośrednictwem inspektora ochrony danych (iod@warszawa.so.gov.pl) lub Samodzielnej Sekcji ds. Zamówień Publicznych (rzp@warszawa.so.gov.pl)

7. Pani/Pana dane osobowe nie będą przetwarzane w celach związanych z automatycznym podejmowanie decyzji w tym w oparciu o profilowanie.