



**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
SPRAWA BBA-2.262.15.2019**

PRZETARG NIEOGRANICZONY

**Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem
dla Urzędu Ochrony Konkurencji i Konsumentów.**

Wartość szacunkowa zamówienia poniżej 144 tys. euro

Zatwierdził:
Maciej Jabłoński

Dyrektor Generalny Urzędu

Warszawa, dnia 10 maja 2019 r.

SPIS TREŚCI

I. Postanowienia ogólne	3
1. Zamawiający	3
2. Tryb i oznaczenie postępowania	3
3. Przedmiot zamówienia	3
4. Termin i miejsce realizacji zamówienia	3
5. Wymagania dotyczące wadium	3
6. Informacja o przewidywanych zamówieniach z art. 67 ust. 1 pkt 6 i 7 ustawy Pzp	5
7. Opis sposobu przygotowania ofert	5
8. Miejsce oraz termin składania i otwarcia ofert	7
9. Opis sposobu udzielania wyjaśnień dotyczących treści niniejszej SIWZ	8
10. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami wraz z określeniem trybu przekazywania oświadczeń i dokumentów	9
11. Termin, do którego Wykonawca będzie związany złożoną ofertą	9
II. Warunki udziału w postępowaniu oraz wymagane dokumenty	9
1. Warunki udziału w postępowaniu	9
2. Wykaz oświadczeń i dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu	10
3. Dokumenty i oświadczenia jakie musi zawierać Oferta	12
III. Procedura postępowania dotycząca wyboru oferty najkorzystniejszej	13
1. Ocena Wykonawców i ofert	13
2. Opis sposobu obliczenia ceny	13
3. Opis kryteriów wyboru najkorzystniejszej oferty wraz z podaniem znaczenia tych kryteriów oraz sposobu oceny ofert	14
IV. Postanowienia końcowe	15
1. Zabezpieczenie należytego wykonania umowy	15
2. Unieważnienie postępowania	15
3. Udzielenie zamówienia	15
4. Istotne postanowienia umowy	15
5. Obowiązujące przepisy	16
6. Informacje o zasadach wprowadzania zmian do zawartej umowy	16
7. Informacja dotycząca przetwarzania danych osobowych	16
V. Pouczenie o środkach ochrony prawnej przysługujących podczas postępowania o udzielenie zamówienia publicznego	17
VI. Załączniki	18

I. POSTANOWIENIA OGÓLNE

1. Zamawiający

Urząd Ochrony Konkurencji i Konsumentów
00 – 950 Warszawa, pl. Powstańców Warszawy 1
telefon: 22 556 01 29, faks: 22 826 20 30
e-mail: zamowienia@uokik.gov.pl
strona internetowa: www.uokik.gov.pl

2. Tryb i oznaczenie postępowania

Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2018 r. poz. 1986 ze zm.), zwanej dalej ustawą Prawo zamówień publicznych lub ustawą Pzp i zostało oznaczone znakiem **BBA-2.262.15.2019**, na jaki Wykonawcy winni się powoływać we wszystkich kontaktach z Zamawiającym.

Zamawiający, zgodnie z art. 24aa ustawy Pzp, zastosuje tzw. procedurę odwróconą, tj. w pierwszej kolejności dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu, tj. zbada oświadczenie wstępne, a następnie zażąda przedłożenia dokumentów w trybie art. 26 ust. 2 ustawy Pzp.

3. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup oraz wymiana sprzętu zapory sieciowej tzw. Firewall'i wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów.

Szczegółowy opis i zakres przedmiotu zamówienia zawarty jest w szczegółowym opisie przedmiotu zamówienia (SOPZ) stanowiącym Załącznik Nr 1 do Specyfikacji Istotnych Warunków Zamówienia (SIWZ) oraz w istotnych postanowieniach umowy stanowiących Załącznik Nr 7 do SIWZ.

Kategoria przedmiotu zamówienia zgodnie ze Wspólnym Słownikiem Zamówień Publicznych (CPV): Kod CPV:

48000000-8 Pakiety oprogramowania i systemy informatyczne
32420000-3 Urządzenia sieciowe

4. Termin i miejsce realizacji zamówienia

Zamawiający wymaga, aby zamówienie zostało zrealizowane w terminie **do 30 dni kalendarzowych od dnia podpisania umowy**.

Miejsce realizacji: siedziba Urzędu Ochrony Konkurencji i Konsumentów w Warszawie, pl. Powstańców Warszawy 1, 00-950 Warszawa.

5. Wymagania dotyczące wadium

- 5.1 Wykonawca jest zobowiązany wnieść wadium w wysokości 3 000,00 zł (słownie złotych: trzy tysiące złotych 00/100).
- 5.2 Wadium może być wniesione w jednej lub kilku następujących formach:
 - a. pieniądzu,

- b. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym,
 - c. gwarancjach bankowych,
 - d. gwarancjach ubezpieczeniowych,
 - e. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 29 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2018, poz. 110).
- 5.3 Wadium wnoszone w pieniądzu należy wpłacić przelewem na następujący rachunek bankowy Zamawiającego: Urząd Ochrony Konkurencji i Konsumentów NBP O/O Warszawa Nr 40 1010 1010 0078 7813 9120 0000, z adnotacją „wadium – numer sprawy BBA-2.262.15.2019” Zaleca się dołączenie do oferty kserokopii dokumentu potwierdzającego dokonanie przelewu.
- 5.4 Za skuteczne wniesienie wadium w pieniądzu, Zamawiający uzna wadium, które znajdzie się na rachunku bankowym Zamawiającego przed upływem terminu składania ofert.
- 5.5 W przypadku wnoszenia wadium w formie gwarancji bankowej lub ubezpieczeniowej, gwarancja musi być gwarancją nieodwołalną, bezwarunkową i płatną na pierwsze pisemne żądanie Zamawiającego, sporządzoną zgodnie z obowiązującymi przepisami i powinna zawierać następujące elementy:
- a. nazwę dającego zlecenie (Wykonawcy), beneficjenta gwarancji (Zamawiającego), gwaranta (banku lub instytucji ubezpieczeniowej udzielających gwarancji) oraz wskazanie ich siedzib,
 - b. kwotę gwarancji,
 - c. termin ważności gwarancji w formule: „od dnia– do dnia”,
 - d. zobowiązanie gwaranta do zapłacenia kwoty gwarancji na pierwsze żądanie Zamawiającego w sytuacjach określonych w art. 46 ust. 4a oraz ust. 5 ustawy Prawo zamówień publicznych,
 - e. Zamawiający nie dopuszcza możliwości umieszczenia w treści gwarancji klauzuli dotyczącej pośrednictwa podmiotów trzecich.
- 5.6 W przypadku wnoszenia wadium w formie innej niż pieniężna, Zamawiający wymaga złożenia wraz z ofertą oryginału dokumentu wadialnego (gwarancji lub poręczenia). Zamawiający zaleca, aby oryginał dokumentu wadialnego nie był trwale połączony z ofertą, w celu umożliwienia zwrotu wadium bez naruszenia oferty.
- 5.7 Wadium musi zabezpieczać ofertę przez cały okres związania ofertą, począwszy od dnia, w którym upływa termin składania ofert.
- 5.8 Zamawiający zwraca wadium wszystkim Wykonawcom niezwłocznie po wyborze oferty najkorzystniejszej lub unieważnieniu postępowania, z wyjątkiem Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, z zastrzeżeniem przypadku określonego w art. 46 ust. 4a ustawy Pzp.
- 5.9 Zamawiający zwraca wadium Wykonawcy, którego oferta została wybrana jako najkorzystniejsza niezwłocznie po zawarciu umowy w sprawie zamówienia publicznego oraz wniesieniu zabezpieczenia należytego wykonania umowy (o ile jest wymagane).
- 5.10 Zamawiający zwraca niezwłocznie wadium, na wniosek Wykonawcy, który wycofał ofertę przed upływem terminu składania ofert.
- 5.11 Zamawiający żąda ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium na podstawie art. 46 ust. 1 ustawy Pzp, jeżeli w wyniku rozstrzygnięcia odwołania jego

oferta została wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez Zamawiającego.

- 5.12 Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a ustawy Pzp, z przyczyn leżących po jego stronie, nie złożył dokumentów lub oświadczeń, potwierdzających okoliczności o których mowa w art. 25 ust. 1 ustawy Pzp, oświadczenia, o którym mowa w art. 25a ust. 1 ustawy Pzp, pełnomocnictw, lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3 ustawy Pzp, co spowodowało brak możliwości wybrania oferty złożonej przez wykonawcę jako najkorzystniejszej.
- 5.13 Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca, którego oferta została wybrana:
- a) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie,
 - b) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.
- 5.14 Zasady wnoszenia wadium określone w niniejszym Rozdziale dotyczą również przedłużania ważności wadium oraz wnoszenia nowego wadium w przypadkach określonych w ustawie.
- 5.15 Zamawiający na podstawie art. 89 ust. 1 pkt 7b ustawy Pzp odrzuci ofertę Wykonawcy, który nie wnieśli wadium w określonym terminie lub wnieśli je w sposób nieprawidłowy w tym również na przedłużony okres związania ofertą lub w sytuacji, o której mowa w art. 46 ust. 3 ustawy Pzp.

6. Informacja o przewidywanych zamówieniach z art. 67 ust. 1 pkt 6 i 7 ustawy Pzp

Zamawiający nie przewiduje udzielenia zamówień w trybie zamówienia z wolnej ręki na podstawie art. 67 ust. 1 pkt 6 i 7 ustawy Pzp.

7. Opis sposobu przygotowania ofert

- 7.1. Wykonawca zobowiązany jest do przedstawienia oferty zgodnie z wymogami SIWZ i ustawy Prawo zamówień publicznych.
- 7.2. Wykonawca może złożyć tylko jedną ofertę.
- 7.3. Dopuszcza się możliwość składania jednej oferty przez dwa lub więcej podmiotów ubiegających się wspólnie o udzielenie zamówienia (np.: konsorcjum).
- 7.4. Zamawiający nie dopuszcza składania ofert wariantowych.
- 7.5. Zamawiający nie dopuszcza składania ofert częściowych.
- 7.6. W przypadku gdy w treści SIWZ zostały użyte nazwy producentów lub modeli, Zamawiający dopuszcza oferowanie urządzeń równoważnych spełniających warunki określone w opisie przedmiotu zamówienia stanowiącym Załącznik Nr 1 do SIWZ.
- 7.7. Oferta oraz pozostałe dokumenty, dla których Zamawiający określił wzory w formie załączników do niniejszej Specyfikacji Istotnych Warunków Zamówienia, winny być sporządzone zgodnie z tymi wzorami co do ich treści.
- 7.8. Oferta oraz dokumenty określone w Części II lit. B i C niniejszej Specyfikacji Istotnych Warunków Zamówienia winny być ze sobą trwale związane.
- 7.9. Oferta winna być sporządzona na piśmie (ręcznie, na maszynie do pisania lub w postaci wydruku komputerowego), w języku polskim, w formie zapewniającej czytelność jej treści. Wszystkie przedkładane dokumenty i oświadczenia winny być sporządzone w języku polskim,

natomiast dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

7.10. Oferta powinna zawierać komplet wymaganych załączników.

7.11. Cenę oferty należy wyrazić w złotych polskich.

7.12. Wszystkie strony oferty zawierające jakąkolwiek treść winny być **podpisane lub zaparafowane przez Wykonawcę**. Wszelkie zmiany w treści oferty (poprawki, przekreślenia, dopiski) powinny być podpisane przez Wykonawcę, natomiast cyfry należy przekreślić i obok napisać prawidłowo – w przeciwnym wypadku nie będą uwzględniane.

7.13. Strony oferty zawierające jakąkolwiek treść winny być kolejno ponumerowane (z zastrzeżeniem sytuacji opisanej w pkt. 7.19). W treści oferty winna być umieszczona informacja o łącznej ilości stron oferty wraz z liczbą i wykazem załączników do oferty.

7.14. Wszystkie dokumenty tworzące ofertę należy przedstawić w formie oryginałów albo kopii poświadczonych za zgodność z oryginałem przez Wykonawcę lub osoby upoważnione do reprezentowania Wykonawcy – z wyłączeniem pełnomocnictw. Poświadczenie za zgodność z oryginałem winno być sporządzone w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczęcią osoby poświadczającej kopię dokumentu za zgodność z oryginałem). W przypadku poświadczania za zgodność z oryginałem kopii dokumentów przez osoby(ę) niewymienione we właściwym rejestrze, należy wraz z ofertą złożyć stosowne pełnomocnictwo.

7.15. Pełnomocnictwo musi zostać złożone w formie oryginału (wystawionego przez osoby wymienione we właściwym rejestrze) lub kserokopii poświadczonych notarialnie.

7.16. Pełnomocnictwo dla podmiotów występujących wspólnie musi być wystawione przez wszystkich wykonawców ubiegających się o udzielenie zamówienia i przedstawione zgodnie z punktem 7.15.

7.17. O ile nie wynika to z innych dokumentów załączonych przez Wykonawcę, do oferty powinno być załączone upoważnienie do jej podpisania.

7.18. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy Prawo zamówień publicznych oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. *Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2018 r. poz. 419 ze zm) rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.*

7.19. W przypadku gdyby oferta zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji **Zamawiający zaleca**, aby informacje zastrzeżone jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa” lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty w sposób niebudzący

wątpliwości, które spośród zawartych w ofercie informacji stanowią taką tajemnicę. Strony zawierające informacje, o których mowa w zdaniu poprzednim, winny być oddzielnie ze sobą połączone, ale ponumerowane z zachowaniem kontynuacji numeracji stron oferty.

- 7.20. Zgodnie z art. 8 ust. 3 z związku z art. 86 ust. 4 ustawy Prawo zamówień publicznych Wykonawca **nie może zastrzec** informacji dotyczących ceny, nazwy (firmy) oraz adresu, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofercie.

8. Miejsce oraz termin składania i otwarcia ofert

- 8.1. Termin składania ofert jest terminem nieprzekraczalnym.
- 8.2. Oferty złożone po terminie zwraca się zgodnie z art. 84 ust. 2 ustawy Prawo zamówień publicznych, natomiast **oferty przesłane faksem nie będą rozpatrywane.**
- 8.3. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty, w tym dostarczenie jej na wskazane miejsce i we wskazanym terminie, odbywa się na koszt i ryzyko Wykonawcy.
- 8.4. **Oferte należy złożyć (dostarczyć)** w siedzibie Zamawiającego w Warszawie (00 – 950), pl. Powstańców Warszawy 1, **Kancelaria pokój nr 1.6 (CSK)**, w dni robocze, w godzinach pracy Zamawiającego, nie później niż **do godziny 11.00 dnia 20 maja 2019 r.**
- 8.5. Ofertę należy umieścić w **podwójnej kopercie (przy czym koperta kurierska nie będzie traktowana jako koperta zewnętrzna)**. Koperty (Zamawiający zaleca, aby koperta zewnętrzna nie była oznaczona nazwą ani logotypem Wykonawcy) należy zaadresować następująco:

✂

Wykonawca:	Zamawiający: Urząd Ochrony Konkurencji i Konsumentów pl. Powstańców Warszawy 1 00-950 Warszawa <u>Wydział Zamówień Publicznych</u>
OFERTA NA: „Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów. Sprawa BBA-2.262.15.2019 Nie otwierać przed dniem 20 maja 2019 r., godz. 11:30	

✂

- 8.6. **Zamawiający nie ponosi odpowiedzialności za przypadkowe otwarcie oferty przetargowej w sytuacji niezgodnego z powyższym sposobu opisanie oferty.**
- 8.7. **Jawne otwarcie ofert nastąpi w dniu 20 maja 2019 r. o godz. 11:30** w siedzibie Zamawiającego w Warszawie, w sali 400, IV piętro.
- 8.8. Bezpośrednio przed otwarciem ofert Zamawiający poda informacje wynikające z art. 86 ust. 3 ustawy Prawo zamówień publicznych, tj. kwotę jaką zamierza przeznaczyć na sfinansowanie zamówienia, a następnie podczas otwarcia ofert informacje wynikające z art. 86

ust. 4 ustawy, tj. nazwy (firmy) oraz adresy Wykonawców, a także informacje dotyczące ceny i warunków płatności zawartych w ofertach.

8.9. **Informacje wskazane w punkcie 8.8 zostaną zamieszczone przez Zamawiającego niezwłocznie po otwarciu ofert na stronie internetowej.**

8.10. Przed upływem terminu składania ofert Wykonawca może wprowadzić zmiany do złożonej oferty lub ją wycofać. Zmiany winny być doręczone Zamawiającemu na piśmie przed upływem terminu składania ofert. Oświadczenie o wprowadzeniu zmian winno być opakowane tak jak oferta, ale opakowanie winno zawierać dodatkowe oznaczenie wyrazem: **ZMIANA lub WYCOFANIE**.

9. Opis sposobu udzielania wyjaśnień dotyczących treści niniejszej SIWZ

9.1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed terminem składania ofert pod warunkiem, że wniosek o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

9.2. Treść zapytań wraz z wyjaśnieniami, bez ujawniania źródła zapytania, Zamawiający przekaże Wykonawcom, którym przekazał Specyfikację Istotnych Warunków Zamówienia oraz zamieści na stronie internetowej, na której została udostępniona SIWZ.

9.3. W uzasadnionych przypadkach, przed upływem terminu składania ofert, Zamawiający może zmienić treść Specyfikacji Istotnych Warunków Zamówienia. Zmiany dokonane przez Zamawiającego zostaną zamieszczone na stronie internetowej na której została udostępniona SIWZ.

9.4. Zmiany mogą wynikać zarówno z pytań zadanych przez Wykonawców, jak i z własnej inicjatywy Zamawiającego.

9.5. Jeżeli zmiana treści SIWZ będzie prowadziła do zmiany treści ogłoszenia o zamówieniu, Zamawiający zamieści ogłoszenie o zmianie ogłoszenia na stronie Biuletynu Zamówień Publicznych.

9.6. Jeżeli w wyniku zmiany treści SIWZ nieprowadzącej do zmiany treści ogłoszenia o zamówieniu będzie niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert i poinformuje o tym Wykonawców, którym przekazano SIWZ oraz zamieści taką informację na stronie internetowej, na której została udostępniona SIWZ.

9.7. Wyjaśnienia, informacja dotycząca przedłużenia terminu składania ofert oraz zmiany treści Specyfikacji Istotnych Warunków Zamówienia, o których mowa w pkt 9.2, 9.3 i 9.5 dodatkowo zostaną zamieszczone na stronie internetowej, na której jest udostępniona Specyfikacja Istotnych Warunków Zamówienia – www.uokik.gov.pl.

9.8. Dokonana przez Zamawiającego zmiana treści Specyfikacji, a także pisemne odpowiedzi na zadane pytania staną się integralną częścią Specyfikacji Istotnych Warunków Zamówienia.

9.9. **Pytania należy kierować do Dyrektora Generalnego Urzędu – Macieja Jabłońskiego na adres, faks lub e-mail wskazany w pkt 1 SIWZ.**

9.10. Osobami upoważnionymi do kontaktowania się z Wykonawcami w zakresie spraw związanych z procedurą postępowania są Przemysław Karpiński lub Artur Krówka, kontakt: zamowienia@uokik.gov.pl.

10. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami wraz z określeniem trybu przekazywania oświadczeń i dokumentów

- 10.1. Oświadczenia, wnioski, zawiadomienia oraz inne informacje Zamawiający i Wykonawcy przekazują pisemnie lub drogą elektroniczną z zastrzeżeniem postanowień pkt 10.2 i 10.3.
- 10.2. Ofertę wraz z załącznikami (również ewentualną ofertę dodatkową), uzupełniane dokumenty w przypadkach określonych w ustawie Prawo zamówień publicznych, Wykonawca składa **w formie pisemnej.**
- 10.3. **W przypadku oświadczeń, dokumentów i pełnomocnictw uzupełnianych w trybie art. 26 ust. 3 Prawo zamówień publicznych nie obowiązuje forma elektroniczna.**
- 10.4. **Jeżeli Zamawiający lub Wykonawcy prześlą oświadczenia, wnioski, zawiadomienia oraz informacje drogą elektroniczną, każda ze stron ma obowiązek niezwłocznie potwierdzić fakt ich otrzymania.**
- 10.5. Publikacja internetowa dokumentacji dotyczącej niniejszego postępowania będzie miała miejsce na stronie www.uokik.gov.pl – publikacja dokumentacji następować będzie tylko w przypadkach przewidzianych ustawą Prawo zamówień publicznych.

11. Termin, do którego Wykonawca będzie związany złożoną ofertą

- 11.1. Termin związania ofertą wynosi 30 dni (zgodnie z art. 85 ust. 1 pkt 1 ustawy Prawo zamówień publicznych). Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.
- 11.2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

II. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ WYMAGANE DOKUMENTY

A. Warunki udziału w postępowaniu

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

- 1.1. nie podlegają wykluczeniu na podstawie art. 24 ust. 1 pkt 12-23 ustawy Prawo zamówień publicznych.
Dodatkowo Zamawiający przewiduje wykluczenie Wykonawcy na podstawie art. 24 ust. 5 pkt 1 ustawy Prawo zamówień publicznych:
 - 1) w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2019 r. poz. 243) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2019 r. poz. 498);
- 1.2. spełniają warunki udziału w postępowaniu, w tym:

1.2.1. posiadają zdolność techniczną i zawodową niezbędną do realizacji zamówienia, Zamawiający uzna ww. warunek za spełniony, jeżeli Wykonawca wykaże, iż:

1.2.1.1. w okresie ostatnich trzech lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie), wykonał a w przypadku dostaw ciągłych wykonuje, co najmniej dwie dostawy polegające na dostawie sprzętu zapory sieciowej wraz z oprogramowaniem, a wartość każdego z tych zamówień wynosiła co najmniej **100 000,00 zł brutto**. W przypadku zamówień nadal wykonywanych faktycznie zrealizowany zakres zamówienia na dzień składania ofert musi spełniać warunki określone powyżej,

1.2.1.2. dysponuje lub będzie dysponował minimum 2 osobami posiadającymi certyfikaty potwierdzające umiejętności obsługi z dostarczonego rozwiązania.

W przypadku konsorcjum lub powoływania się na zasoby podmiotów trzecich wymagane jest aby warunki określone w pkt. 1.2.1.1. spełniał w całości co najmniej jeden z wykonawców lub podmiot trzeci na zasoby, którego Wykonawca powołuje się w celu wykazania spełnienia warunków udziału w postępowaniu.

B. Wykaz oświadczeń i dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu

1. Wszyscy Wykonawcy są zobowiązani złożyć:

- **do oferty** - aktualne na dzień składania ofert oświadczenia, o których mowa w art. 25a ust. 1 ustawy Prawo zamówień publicznych:

1.1. oświadczenie o niepodleganiu wykluczeniu z postępowania w zakresie określonym w pkt 1.1. lit. A Części II SIWZ (Załącznik Nr 2 do SIWZ),

1.2. oświadczenie o spełnianiu warunków udziału w postępowaniu w zakresie określonym w pkt 1.2. lit. A Części II SIWZ (Załącznik Nr 3 do SIWZ),

- **po otwarciu ofert**

1.3. oświadczenie o przynależności (wzór oświadczenia Załącznik Nr 4 do SIWZ) lub braku przynależności (wzór oświadczenia Załącznik Nr 4A do SIWZ) do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Prawo zamówień publicznych - w terminie 3 dni od zamieszczenia na stronie internetowej Zamawiającego informacji z otwarcia ofert, o której mowa w pkt 8.8 Części I SIWZ.

2. Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia przekazania wezwania, aktualnych na dzień złożenia oświadczeń i dokumentów potwierdzających okoliczności, o których mowa w pkt 1.1. i 1.2. lit. A Części II SIWZ, tj.:

2.1. Odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 5 pkt 1 ustawy Prawo zamówień publicznych,

- **w zakresie spełniania warunków udziału, określonych w pkt 1.2. lit. A Części II SIWZ**

2.2. Wykazu dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane oraz załączeniem dowodów określających czy te zamówienia zostały wykonane lub są wykonywane należycie - potwierdzający spełnianie warunku określonego w pkt 1.2. lit. A Części II SIWZ (wypełniony i podpisany Załącznik Nr 6 do SIWZ).

Podane wartości muszą dotyczyć jednego zamówienia (przez co rozumie się, że musi wynikać z jednostkowej umowy).

Dowodami, o których mowa powyżej są:

- referencje bądź inne dokumenty wystawione przez podmiot na rzecz którego dostawy lub usługi były wykonywane lub są wykonywane, z tym, że w odniesieniu do nadal wykonywanych dostaw lub usług okresowych lub ciągłych referencje lub inne dokumenty powinny być wydane nie wcześniej niż na 3 miesiące przed upływem terminu składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu;
- w przypadku usług lub dostaw – inne dokumenty – jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów o których mowa powyżej.

Dokumenty muszą być wystawione przez Zamawiającego zamówienie/ Odbiorcę zamówienia.

2.3. Wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie dysponowania tymi osobami - potwierdzający spełnianie warunku określonego w pkt 1.2.1.2. lit. A Części II SIWZ (wypełniony i podpisany Załącznik Nr 8 do SIWZ).

W przypadku Wykonawców ubiegających się wspólnie o udzielenie zamówienia warunek udział w postępowaniu, określony w pkt 1.2.1 lit. A Części II SIWZ musi spełniać samodzielnie przynajmniej jeden z Wykonawców (członków konsorcjum)

3. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach lub w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.

W powyższym przypadku, Wykonawca musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając w tym celu zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

W przypadku, gdy Wykonawca wykazując spełnianie warunków udziału w postępowaniu, o których mowa w pkt 1.2. lit. A Części II SIWZ polega na zasobach innych podmiotów na zasadach określonych w art. 22 a ust. 1 ustawy Prawo zamówień publicznych, Wykonawca jest zobowiązany zamieścić informacje o tym podmiocie w oświadczeniu o niepodleganiu wykluczeniu z postępowania (Załącznik Nr 2 do SIWZ) oraz w oświadczeniu o spełnianiu warunków udziału w postępowaniu (Załącznik Nr 3 do SIWZ). W przypadku, gdy oferta Wykonawcy powołującego się na zasoby innych podmiotów zostanie najwyższej oceniona, taki Wykonawca będzie zobowiązany do przedstawienia w odniesieniu do tych podmiotów dokumentów, o których mowa w pkt 2.1 lit. B Części II SIWZ. W przypadku gdy oferta Wykonawcy powołującego się na zasoby innych podmiotów zostanie najwyższej oceniona, taki Wykonawca będzie zobowiązany do przedstawienia w odniesieniu do tych podmiotów następujących dokumentów:

- a) aktualnego na dzień złożenia, odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 5 pkt 1 ustawy Prawo zamówień publicznych.

W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi lub dostawy, do realizacji których te zdolności są wymagane.

C. Dokumenty i oświadczenia jakie musi zawierać Oferta

1. Prawidłowo wypełniony i podpisany: Formularz Ofertowy (Załącznik Nr 5 do SIWZ).
2. Oświadczenia wymienione w pkt 1.1. i 1.2 lit. B Części II SIWZ.
3. Oryginał pełnomocnictwa do złożenia oferty lub kopia pełnomocnictwa potwierdzona przez mocodawcę lub notariusza, o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą. Przyjmuje się, że pełnomocnictwo do złożenia oferty upoważnia również do poświadczenia za zgodność z oryginałem kopii wszystkich dokumentów składanych wraz z ofertą, chyba że z treści pełnomocnictwa wynika co innego.
4. Oświadczenie czy wybór oferty Wykonawcy będzie prowadził do powstania u Zamawiającego obowiązku podatkowego – Wykonawca może zamieścić niniejsze oświadczenie w Formularzu ofertowym lub też w odrębnym dokumencie.
5. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego – Wykonawcy zobowiązani są złożyć stosowne pełnomocnictwo (stanowiące oświadczenie każdego z podmiotów) wystawione zgodnie z dyspozycją zawartą w pkt 7.15 i 7.16 Części I SIWZ.

W przypadku Wykonawców występujących wspólnie o udzielenie zamówienia obowiązują następujące zasady składania dokumentów:

- a) każdy z uczestników wchodzący w skład podmiotu wspólnie ubiegającego się o udzielenie zamówienia musi wraz z ofertą złożyć oświadczenia wymienione w pkt 1.1 - 1.2 lit. B Części II SIWZ,
- b) każdy z uczestników wchodzący w skład podmiotu wspólnie ubiegającego się o udzielenie zamówienia musi złożyć oświadczenia i dokumenty wymienione w pkt 1.3 lit. B Części II SIWZ oraz w pkt 2.1 lit. B Części II SIWZ,
- c) wszystkie dokumenty Wykonawców mogących wspólnie ubiegać się o udzielenie zamówienia muszą wchodzić w skład danej oferty i być złożone łącznie,
- d) dokument wskazany w pkt 2.2 lit. B Części II SIWZ musi zostać złożony w taki sposób aby wskazywał, iż warunek spełnia w całości co najmniej jeden z konsorcjantów lub też podmiot trzeci na zasoby którego wykonawca się powołuje,
- e) jeżeli oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, zostanie wybrana, taki Wykonawca będzie zobowiązany przed zawarciem umowy w sprawie zamówienia publicznego do złożenia Zamawiającemu umowy regulującej współpracę tych Wykonawców,
- f) wspólnicy spółki cywilnej są traktowani jak Wykonawcy składający ofertę wspólną i mają do nich zastosowanie zasady określone powyżej.

III. PROCEDURA POSTĘPOWANIA DOTYCZĄCA WYBORU OFERTY NAJKORZYSTNIEJSZEJ

1. Ocena Wykonawców i ofert

- 1.1. Jeżeli Wykonawca w określonym terminie nie złożył oświadczenia o którym mowa w art. 25 a ust. 1 ustawy Pzp, oświadczeń lub dokumentów wymaganych przez Zamawiającego na potwierdzenie warunków, o których mowa w art. 25 ust. 1, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielenia wyjaśnień w wyznaczonym terminie, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
- 1.2. Jeżeli Wykonawca w określonym terminie nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wzywa do ich złożenia w wyznaczonym terminie, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
- 1.3. Zamawiający może wezwać Wykonawców do złożenia, w wyznaczonym przez siebie terminie, wyjaśnień dotyczących oświadczeń lub dokumentów, o których mowa w art. 25 ust. 1 ustawy Prawo zamówień publicznych.
- 1.4. Zapisy pkt 1.1 stosuje się odpowiednio do listy podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Prawo zamówień publicznych, albo informacji o tym, iż Wykonawca nie należy do tej samej grupy kapitałowej.
- 1.5. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
- 1.6. Zamawiający poprawi w ofercie:
 - a. oczywiste omyłki pisarskie
 - b. oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek
 - c. inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty- niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona
- 1.7. Zamawiający może wezwać Wykonawcę do złożenia w wyznaczonym terminie wyjaśnień dotyczących wyliczenia ceny lub kosztu w celu ustalenia, czy zaoferowana cena lub koszt lub ich istotne części składowe zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.
- 1.8. Zamawiający powiadomi na piśmie o wyniku postępowania wszystkich Wykonawców, którzy złożyli oferty oraz zamieści informacje określone w art. 92 ust. 1 pkt 1 ustawy Prawo zamówień publicznych na stronie internetowej Zamawiającego.

2. Opis sposobu obliczenia ceny

- 2.1. Wykonawca w Formularzu ofertowym ustala wynagrodzenie ryczałtowe, za cały zakres rzeczowy określony w Załączniku Nr 1 do SIWZ. Wynagrodzenie to będzie stanowić całkowite wynagrodzenie Wykonawcy, uwzględniające wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z SIWZ.
- 2.2. W formularzu ofertowym należy wskazać: cenę ryczałtową brutto za wykonanie przedmiotu zamówienia uwzględniającą podatek VAT w obowiązującej stawce, ceny jednostkowe za dostawę sprzętu zapory sieciowej oraz cenę za oprogramowanie.

- 2.3. Wykonawca, dokonując kalkulacji warunków cenowych swoich ofert jest zobowiązany do przestrzegania zasad uczciwej konkurencji z zastrzeżeniem, iż cena lub koszt lub ich istotne części składowe nie mogą być rażąco niskie w stosunku do przedmiotu zamówienia. Konsekwencją złożenia oferty z rażąco niską ceną lub kosztem jest jej odrzucenie – zgodnie z art. 89 ust. 1 pkt 4 w związku z art. 90 ust. 3 ustawy Pzp.
- 2.4. Wykonawca w przedstawionej ofercie winien zaoferować cenę kompletną, jednoznaczną, i ostateczną. Ewentualne upusty oferowane przez Wykonawcę winny być uwzględnione w cenie oferty.
- 2.5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca składając ofertę informuje Zamawiającego (składając oświadczenie w Formularzu ofertowym lub w innym oświadczeniu), czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez podatku VAT.
- 2.6. Rozliczenia między Wykonawcą a Zamawiającym dokonywane będą w PLN. Zamawiający nie dopuszcza możliwości prowadzenia z Wykonawcą rozliczeń w innej walucie niż PLN.
- 2.7. Wykonawca określa cenę oferty z dokładnością dwóch miejsc po przecinku.

3. Opis kryteriów wyboru najkorzystniejszej oferty wraz z podaniem znaczenia tych kryteriów oraz sposobu oceny ofert

- 3.1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert:

- **Cena oferty (X) - 60% (waga kryterium)**

- **Gwarancja roczna i serwis producenta na poziomie 24x7 – 40% (waga kryterium)**

Cena oferty (X) - 60% (waga kryterium)

W ramach kryterium cena oferty ocena ofert będzie dokonywana według następującej zasad: do oceny poszczególnych ofert w zakresie **kryterium cena oferty** zostanie zastosowana metoda polegająca na porównaniu ceny badanej oferty z najtańszą spośród cen przedstawionych przez tych Wykonawców, których oferty zostały dopuszczone do oceny i spełniają warunki określone w Specyfikacji. Jako cenę oferty przyjmuje się wartość brutto podaną w Formularzu Ofertowym.

Punkty będą liczone według wzoru:

$$X = \frac{C_n}{C_b} \times 60 \text{ (waga kryterium)}$$

X – liczba punktów w ramach kryterium ceny (obliczana do dwóch miejsc po przecinku)

C_n – najniższa cena ofertowa brutto spośród ocenianych ofert

C_b – cena brutto oferty ocenianej

Gwarancja roczna i serwis producenta na poziomie 24x7 (G) – 40% (waga kryterium)

W ramach kryterium gwarancja roczna i serwis producenta na poziomie 24x7 maksymalna ilość punktów tj. 40 pkt będzie przyznana za zaoferowanie 12 miesięcznej gwarancji i serwisu producenta w zakresie 24hx7 dni w tygodniu na całość oferowanego rozwiązania.

3.2. Łączna ilość punktów dla badanej oferty będzie liczona wg następującego wzoru:

$$S = X + G$$

gdzie: S – łączna suma punktów badanej oferty.

3.3. Przyjmuje się, że 1% = 1 pkt.

3.4. Wykonawca, który uzyska najwyższą łączną ilość punktów i będzie spełniał wszystkie warunki określone w Specyfikacji Istotnych Warunków Zamówienia oraz ustawie Prawo zamówień publicznych zostanie wybrany do realizacji zamówienia.

IV. POSTANOWIENIA KOŃCOWE

1. Zabezpieczenie należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

2. Unieważnienie postępowania

Zamawiający unieważni postępowanie w przypadkach określonych w art. 93 ust. 1 ustawy Pzp.

3. Udzielenie zamówienia

3.1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wymaganiom określonym w ustawie Pzp, niniejszej SIWZ oraz została uznana za najkorzystniejszą.

3.2. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający ogłosi wyniki postępowania.

3.3. Zamawiający zawrze umowę w sprawie zamówienia publicznego zgodnie z dyspozycją art. 94 ustawy Pzp. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą jest zobowiązany do stawienia się w celu podpisania w terminie i miejscu wskazanym przez Zamawiającego.

3.4. Jeżeli Wykonawca, którego oferta została wybrana, uchyli się od zawarcia umowy, Zamawiającemu przysługuje prawo wyboru oferty najkorzystniejszej spośród pozostałych ofert, bez przeprowadzania ich ponownego badania i oceny chyba, że zachodzą przesłanki do unieważnienia postępowania.

3.5. W przypadku uznania za najkorzystniejszą oferty Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający przed podpisaniem umowy zażąda umowy regulującej współpracę tych podmiotów, jako warunek niezbędny zawarcia umowy o udzielenie zamówienia publicznego.

3.6. Zasady współpracy podmiotów występujących wspólnie muszą być zgodne z dyspozycjami ustawy Prawo zamówień publicznych, w szczególności podmioty te ponoszą solidarną odpowiedzialność za wykonanie umowy.

4. Istotne postanowienia umowy

Postanowienia umowy oraz zasady współpracy pomiędzy wybranym do realizacji zamówienia Wykonawcą a Zamawiającym określają Istotne postanowienia umowy stanowiące **Załącznik Nr 7 do SIWZ**.

5. Obowiązujące przepisy

W kwestiach, które nie zostały wyjaśnione w niniejszej SIWZ zastosowanie mają przepisy ustawy Prawo zamówień publicznych wraz z aktami wykonawczymi wydanymi na jej podstawie oraz Kodeks cywilny.

6. Informacje o zasadach wprowadzania zmian do zawartej umowy

Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonany zostanie wybór, w trybie art. 144 ust. 1 ustawy Pzp, w zakresie i na warunkach określonych w **Załączniku Nr 7 do SIWZ – Istotne postanowienia umowy**.

7. Informacja dotycząca przetwarzania danych osobowych

Zgodnie z art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej RODO), informujemy, że:

Administratorem jest Prezes Urzędu Ochrony Konkurencji i Konsumentów z siedzibą w Warszawie (00-950), pl. Powstańców Warszawy 1.

Inspektor ochrony danych jest dostępny za pomocą środków komunikacji elektronicznej: iod@uokik.gov.pl.

Cele przetwarzania danych osobowych

UOKiK przetwarza Pani/Pana dane osobowe, w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego.

Podstawa prawna przetwarzania danych

Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (podstawa prawna z art. 6 ust. 1 lit. c RODO) oraz ustawy Pzp.

Informacje o odbiorcach danych osobowych

Dane osobowe Pana/Pani mogą być udostępnione osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania, w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp.

Okres, przez który dane osobowe będą przechowywane

Dane będą przechowywane 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.

Uprawnienia z art. 15-21 ogólnego rozporządzenia o ochronie danych:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO**.

Nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Prawo do wniesienia skargi

Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych przez Administratora narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Podstawa podania danych osobowych

Podanie przez Pana/Panią swoich danych osobowych jest wymogiem ustawowym. Obowiązek podania danych przez Pana/Panią wynika z ustawy Pzp, związanych z udziałem w postępowaniu o udzielenie zamówienia publicznego.

Informacja o zautomatyzowanym podejmowaniu decyzji

Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym w oparciu o profilowanie.

** **Wyjaśnienie:** skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

*** **Wyjaśnienie:** prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

V. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH PODCZAS POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO

1. Przepisy ogólne

- 1.1. Środki ochrony prawnej przewidziane w dziale VI (art. 179-198g) ustawy Prawo zamówień publicznych, przysługują Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy.
- 1.2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy Prawo zamówień publicznych.
- 1.3. Środkami ochrony prawnej, o których mowa w pkt 1 są:
 - odwołanie do Prezesa Krajowej Izby Odwoławczej;
 - skarga do sądu

2. Odwołanie

- 2.1. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której zamawiający jest zobowiązany na podstawie ustawy Prawo zamówień publicznych.

- 2.2. Odwołanie wnosi się do Prezesa Izby w terminach określonych w art. 182 ustawy Prawo zamówień publicznych, w formie pisemnej albo elektronicznej opatrzonej bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu.
- 2.3. W przypadku wniesienia odwołania po upływie terminu składania ofert, bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Izbę orzeczenia.
- 2.4. Izba rozpoznaje odwołanie w terminie 15 dni od jego doręczenia Prezesowi Izby
- 2.5. Dla niniejszego postępowania mają zastosowanie przepisy odpowiednie dla postępowań, których wartość zamówienia nie przekracza równowartości kwoty określonej w art. 11 ust. 8 ustawy Pzp w związku z czym odwołanie przysługuje wyłącznie wobec czynności:
- a) wyboru trybu negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę;
 - b) określenia warunków udziału w postępowaniu;
 - c) wykluczenia odwołującego z postępowania o udzielenie zamówienia;
 - d) odrzucenia oferty odwołującego;
 - e) opisu przedmiotu zamówienia;
 - f) wyboru najkorzystniejszej oferty.

3. Skarga do sądu

- 3.1. Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
- 3.2. Skargę wnosi się do sądu okręgowego właściwego dla siedziby albo miejsca zamieszkania Zamawiającego, za pośrednictwem Prezesa Urzędu w terminie 7 dni od dnia doręczenia orzeczenia Izby, przesyłając jednocześnie jej odpis przeciwnikowi skargi.
- 3.3. Sąd rozpoznaje skargę niezwłocznie, nie później jednak niż w terminie 1 miesiąca od dnia wpłynięcia skargi do sądu.
- 3.4. Od wyroku sądu lub postanowienia kończącego postępowania w sprawie, nie przysługuje skarga kasacyjna. Przepisu nie stosuje się do Prezesa Urzędu.

VI. ZAŁĄCZNIKI

1. Załącznik Nr 1 – Szczegółowy opis przedmiotu zamówienia
2. Załącznik Nr 2 – Oświadczenie o przesłankach podleganiu wykluczeniu z postępowania
3. Załącznik Nr 3 – Oświadczenie o spełnianiu warunków udziału w postępowaniu
4. Załącznik Nr 4 – Oświadczenie o przynależności do grupy kapitałowej
5. Załącznik Nr 4A – Oświadczenie o braku przynależności do grupy kapitałowej
6. Załącznik nr 5 – Formularz Ofertowy
7. Załącznik Nr 6 – Wykaz usług
8. Załącznik Nr 7 – Istotne postanowienia umowy
9. Załącznik Nr 8 - Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia

**Szczegółowy opis przedmiotu zamówienia
(sprawa BBA-2.262.15.2019)**

Przedmiotem zamówienia jest wymiana urządzeń firmy FortiNet wchodzących w skład infrastruktury sieciowej i bezpieczeństwa Zamawiającego oraz zakup oprogramowania do zarządzania i analizy wymienionymi urządzeniami w Urzędzie Ochrony Konkurencji i Konsumentów (Plac Powstańców Warszawy 1, Warszawa) wraz z usługą wymiany i konfiguracji.

1. Zamawiający posiada następujące urządzenia podlegające wymianie:

- a) FortiGate 60D – 18 szt.
- b) FortiGate 100D – 2 szt.

Szczegółowe dane urządzeń:

Producent	Model	Numer Seryjny
Fortigate	100D	FG100D3G16810254
Fortigate	100D	FG100D3G16810248
Fortigate	60D	FGT60D4Q16016018
Fortigate	60D	FGT60D4Q16015618
Fortigate	60D	FGT60D4Q16016029
Fortigate	60D	FGT60D4Q16015439
Fortigate	60D	FGT60D4Q16016031
Fortigate	60D	FGT60D4Q16015835
Fortigate	60D	FGT60D4Q16015296
Fortigate	60D	FGT60D4Q16015804
Fortigate	60D	FGT60D4Q16015192
Fortigate	60D	FGT60D4Q16015806
Fortigate	60D	FGT60D4Q16015952
Fortigate	60D	FGT60D4Q16015422
Fortigate	60D	FGT60D4Q16015441
Fortigate	60D	FGT60D4Q16015979

Fortigate	60D	FGT60D4Q16015975
Fortigate	60D	FGT60D4Q16016063
Fortigate	60D	FGT60D4Q16015454
Fortigate	60D	FGT60D4Q16015217

Powyższe urządzenia użytkowane są w:

- a) FortiGate 100D – 2 szt. – siedziba Zamawiającego
- b) FortiGate 60D – 18 szt. – jednostki zamiejscowe Zamawiającego

2. Dostarczone rozwiązanie musi spełniać wymagania wskazane w punktach dla wymienionych urządzeń:
 - FortiGate 100D – 2 szt. – wymiana do 2 sztuk urządzeń opisanych w punkcie **Urządzenie A**
 - FortiGate 60D – 18 szt. – wymiana do 18 sztuk urządzeń opisanych w punkcie **Urządzenie B**
 - Centralne zarządzanie dostarczonymi urządzeniami – opisane w punkcie **System centralnego zarządzania urządzeniami bezpieczeństwa**

Dostarczone urządzenia w ilości 18 szt. które przeznaczone są do jednostek zamiejscowych Zamawiającego muszą zostać w pełni skonfigurowane wraz z urządzeniami przeznaczonymi do instalacji w siedzibie Zamawiającego przez osoby wyznaczone przez Wykonawcę do realizacji zamówienia na miejscu w siedzibie Zamawiającego.

3. Po wymianie urządzenia muszą spełniać następujące minimalne parametry techniczne:

3.1 Urządzenie A (platforma sprzętowa)

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 musi pochodzić z oficjalnej dystrybucji producenta.

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, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

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. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

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

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 8 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.2 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 820 Mbps.

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 - zaporą ogniową klasy Stateful Inspection.

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 - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
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 protokołem 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) dla protokołu 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/Counter Mode(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.
3. Oferowane urządzenia muszą umożliwiać dwuetapową autoryzację dla minimum 200 użytkowników. Autoryzacja ta musi zapewniać:
- Zgodność z OATH, wsparcie dla urządzeń mobilnych dla tokenów generowanych zgodnie z TOTP (algorytm Time-based One-time Password) oraz HOTP (algorytm HMAC-based One-time Password.)
 - Wsparcie dla aplikacji generującej tokeny co najmniej dla platform: iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10 i Windows Universal Platform
 - Aplikacja musi wspierać następujące funkcje:
 - Samo-kasowanie w przypadku ataku brut-force
 - Kopiowanie generowanego tokena do schowka
 - Zabezpieczenie poprzez PIN i odcisk palca

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. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 6500 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. System musi dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
7. 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.
8. 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 2500 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 40 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, proxy.
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. 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:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel 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. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
2. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
- 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 przez okres minimum 12 miesięcy. Powinny one obejmować:

- Kontrolę aplikacji,
- IPS,
- Antywirus,
- Antyspam,
- Web Filtering
- Ochrona systemów przemysłowych SCADA

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 minimalnie w trybie 8x5.

3.2 Urządzenie B (platforma sprzętowa)

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 musi pochodzić z oficjalnej dystrybucji producenta.

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, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

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.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
 - 10 portami Gigabit Ethernet RJ-45.
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 musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 30000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 2 Gbps.
5. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 135 Mbps.

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 - zaporą ogniową klasy Stateful Inspection.
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 - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
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.

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) dla protokołu 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/Counter Mode(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. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 6500 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 2500 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 40 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, proxy.
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. 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:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel 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. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
- 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 przez okres minimum 12 miesięcy. Powinny one obejmować:

- Kontrolę aplikacji,
- IPS,
- Antywirus,
- Antyspam,
- Web Filtering
- Ochrona systemów przemysłowych SCADA

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 minimum w trybie 8x5.

3.3 System centralnego zarządzania urządzeniami bezpieczeństwa.

W ramach postępowania wymagany jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego (np. NGFW).

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy lub komercyjnych platform działających w środowisku wirtualnym lub w postaci komercyjnej platformy/komercyjnych platform działających na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM.

Interfejsy, Dyski:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 200 GB.

Parametry wydajnościowe:

1. System musi umożliwiać zarządzanie co najmniej 20 systemami bezpieczeństwa.
2. System musi być w stanie przyjmować minimum 2 GB logów na dzień.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 20 systemów.

Funkcje systemu centralnego zarządzania

W ramach centralnego systemu zarządzania muszą być realizowane co najmniej poniższe funkcje:

1. System musi posiadać system zarządzania zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).
2. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3. System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4. System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
5. System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
6. System musi umożliwiać zarządzanie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.

7. System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8. System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
10. System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach.
11. System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).
12. System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mesh.
13. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

Funkcje logowania

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.

Funkcja raportowania

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. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Funkcje korelacji

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.
 - a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.
2. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
3. System musi posiadać API które umożliwia zarządzanie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.
4. Powinna istnieć możliwość zdefiniowania co najmniej 5 lokalnych kont administracyjnych.

Gwarancja oraz wsparcie

Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego minimum w trybie 8x5.

3.4 System centralnego zarządzania urządzeniami bezpieczeństwa i analizy.

W ramach postępowania wymagany jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego (np. NGFW).

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy lub komercyjnych platform działających w środowisku wirtualnym lub w postaci komercyjnej platformy/komercyjnych platform działających na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM. Rozwiązanie musi umożliwić rozdzielenie funkcji zarządzania i raportowania/analizy.

Interfejsy, Dyski:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 200 GB dla systemu zarządzania i co najmniej 500GB dla systemu analizy i monitorowania.

Parametry wydajnościowe:

4. System musi umożliwiać zarządzanie co najmniej 20 systemami bezpieczeństwa.
5. System musi być w stanie przyjmować minimum 2 GB logów na dzień (zarówno dla systemu zarządzania i monitorowania).
6. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 20 systemów.

Funkcje systemu centralnego zarządzania

W ramach centralnego systemu zarządzania muszą być realizowane co najmniej poniższe funkcje:

1. System musi posiadać system zarządzania zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).
2. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3. System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4. System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
5. System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
6. System musi umożliwiać zarządzanie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.
7. System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8. System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
10. System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach.
11. System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).
12. System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mesh.
13. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

Funkcje logowania

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.

Funkcja raportowania

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. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Funkcje korelacji

W zakresie korelacji zdarzeń system zarządzania i analizy 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.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI
3. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
4. System musi posiadać API które umożliwia zarządzanie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.
5. Powinna istnieć możliwość zdefiniowania co najmniej 5 lokalnych kont administracyjnych.

Gwarancja oraz wsparcie

Wsparcie: System zarządzania i monitorowania musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego minimum w trybie 8x5.

Zamawiający:

**Urząd Ochrony Konkurencji
i Konsumentów**

pl. Powstańców Warszawy 1
00-950 Warszawa

Wykonawca:

.....
.....

*(pełna nazwa/firma, adres, w
zależności od podmiotu: NIP/PESEL,
KRS/CEiDG)*

reprezentowany przez:

.....
.....

*(imię, nazwisko, stanowisko/podstawa
do reprezentacji)*

Oświadczenie Wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.
Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów.** (nr post. BBA-2.262.15.2019), prowadzonego przez Urząd Ochrony Konkurencji i Konsumentów, oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-23 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp.

....., dnia r.

(miejscowość)

.....

(podpis)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:

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

....., dnia r.

(miejscowość)

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, 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 podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

....., dnia r.

(miejscowość)

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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 r.

(miejscowość)

(podpis)

Zamawiający:

**Urząd Ochrony Konkurencji
i Konsumentów**

pl. Powstańców Warszawy 1
00-950 Warszawa

Wykonawca:

.....
.....

*(pełna nazwa/firma, adres, w
zależności od podmiotu: NIP/PESEL,
KRS/CEiDG)*

reprezentowany przez:

.....
.....

*(imię, nazwisko, stanowisko/podstawa
do reprezentacji)*

Oświadczenie Wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów.** (nr post. BBA-2.262.15.2019), prowadzonego przez Urząd Ochrony Konkurencji i Konsumentów, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w pkt 1.2 lit. A Części II SIWZ.

....., dnia r.

(miejscowość)

.....

(podpis)

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w (wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu), polegam na zasobach następującego/ych podmiotu/ów:

.....
.....,
w następującym zakresie..... (wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

....., dnia r.
(miejscowość) (podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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 r.
(miejscowość) (podpis)

Zamawiający:

**Urząd Ochrony Konkurencji
i Konsumentów**

pl. Powstańców Warszawy 1
00-950 Warszawa

Wykonawca:

.....
.....

*(pełna nazwa/firma, adres, w
zależności od podmiotu: NIP/PESEL,
KRS/CEiDG)*

reprezentowany przez:

.....
.....

*(imię, nazwisko, stanowisko/podstawa
do reprezentacji)*

Oświadczenie Wykonawcy

składane na podstawie art. 24 ust. 11 ustawy z dnia 29 stycznia 2004 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów.** (nr post. BBA-2.262.15.2019), prowadzonego przez Urząd Ochrony Konkurencji i Konsumentów, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

po zapoznaniu się z informacją z otwarcia ofert zamieszczoną przez Zamawiającego na stronie internetowej oświadczam, **że należę do tej samej grupy kapitałowej** o której mowa art. 24 ust. 1 pkt 23 ustawy Pzp, w skład której wchodzi/ą Wykonawca/y, który/rzy złożył/li ofertę:

1.
2.

3.
4.

Jednocześnie oświadczam, że w związku z ww. okolicznością, przedstawiam następujące informacje i dowody, że powiązania z ww. podmiotami nie prowadzą do zakłócenia konkurencji w niniejszym postępowaniu:

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

....., dnia r.

(miejscowość)

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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 r.

(miejscowość)

.....

(podpis)

Zamawiający:

**Urząd Ochrony Konkurencji
i Konsumentów**

pl. Powstańców Warszawy 1
00-950 Warszawa

Wykonawca:

.....
.....

*(pełna nazwa/firma, adres, w
zależności od podmiotu: NIP/PESEL,
KRS/CEiDG)*

reprezentowany przez:

.....
.....

*(imię, nazwisko, stanowisko/podstawa
do reprezentacji)*

Oświadczenie Wykonawcy

składane na podstawie art. 24 ust. 11 ustawy z dnia 29 stycznia 2004 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE BRAKU PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów.** (nr post. BBA-2.262.15.2019), prowadzonego przez Urząd Ochrony Konkurencji i Konsumentów, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

po zapoznaniu się z informacją z otwarcia ofert zamieszczoną przez Zamawiającego na stronie internetowej oświadczam, że **nie należę do tej samej grupy kapitałowej** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2019 r., poz. 369 ze zm.), w skład której wchodzi inny Wykonawca, który złożył ofertę w przedmiotowym postępowaniu.

....., dnia r.

(miejscowość)

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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 r.

(miejscowość)

.....

(podpis)

.....
 (nazwa i adres Wykonawcy pieczęć)
 Tel.
 Faks.
 REGON
 NIP

Urząd Ochrony Konkurencji i Konsumentów
pl. Powstańców Warszawy 1
00-950 Warszawa

FORMULARZ OFERTOWY

(sprawa BBA-2.262.15.2019)

W odpowiedzi na publiczne ogłoszenie o zamówieniu publicznym prowadzonym w trybie przetargu nieograniczonego na **Zakup oraz wymiana sprzętu zapory sieciowej wraz z oprogramowaniem dla Urzędu Ochrony Konkurencji i Konsumentów**, oświadczam, że oferujemy wykonanie przedmiotu zamówienia w zakresie określonym w Specyfikacji Istotnych Warunków Zamówienia, zgodnie z opisem przedmiotu zamówienia na następujących warunkach cenowych:

Cena za wykonanie całości przedmiotu zamówienia: **zł brutto.**
(słownie złotych:)

w tym:

Przedmiot zamówienia	Liczba sztuk	Cena jednostkowa brutto w PLN	Wartość brutto w PLN
A	B	C	D = B * C
Urządzenia A (marka) (model)	2		
Urządzenia B (marka) (model)	18		
Oprogramowanie do zarządzania i analizy urządzeń	1	Wartość brutto w PLN	
			

(nazwa)		
..... (wersja)		

Oświadczamy, iż udzielamy 12 miesięcy gwarancji wraz z serwisem producenta w zakresie 24h x 7 dni w tygodniu na całość oferowanego rozwiązania na warunkach określonych w SIWZ - TAK/NIE.*

Oświadczam/y, że powyższe ceny brutto zawierają wszystkie koszty, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.

Oświadczamy, iż oferowane urządzenia oraz system zarządzania spełniają wszystkie wymagania Zamawiającego określone w Załączniku Nr 1 do SIWZ „Szczegółowy opis przedmiotu zamówienia”.

W trybie art. 91 ust. 3a ustawy Prawo zamówień publicznych **oświadczamy, iż** wybór naszej oferty **nie będzie/będzie *** prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy o podatku od towarów i usług.¹

*(*niewłaściwe skreślić)*

(¹wybór oferty Wykonawcy prowadzi do „powstania u Zamawiającego obowiązku podatkowego”, kiedy zgodnie z przepisami ustawy o podatku od towarów i usług to nabywca (Zamawiający) będzie zobowiązany do rozliczenia (odprowadzenia) podatku VAT, co może mieć miejsce w przypadku:

- wewnątrzwspólnotowego nabycia towarów,*
- importu usług lub towarów,*
- mechanizmu odwróconego obciążenia podatkiem VAT.)*

*W przypadku, gdy wybór oferty Wykonawcy **będzie prowadził** do powstania u Zamawiającego obowiązku podatkowego Wykonawca zobowiązany jest wskazać nazwę (rodzaj) towaru lub usług, wartość tego towaru lub usług bez kwoty podatku VAT.*

Nazwa towaru lub usług prowadzących do powstania u Zamawiającego obowiązku podatkowego

*.....
oraz wartość tych towarów i usług bez podatku od towarów i usług: zł*

UWAGA! Powyższe pola zaznaczone kursywą wypełniają wyłącznie Wykonawcy, których wybór oferty prowadziłby u Zamawiającego do powstania obowiązku podatkowego tzn. kiedy zgodnie z przepisami ustawy o podatku od towarów i usług to nabywca (Zamawiający) będzie zobowiązany do rozliczenia (odprowadzenia) podatku VAT

Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w Specyfikacji Istotnych Warunków Zamówienia tj. 30 dni od terminu składania ofert.

Oświadczamy, że naszym pełnomocnikiem dla potrzeb niniejszego zamówienia jest:
.....

(Wypełniają jedynie przedsiębiorcy składający wspólną ofertę)

Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia i nie wnosimy do niej zastrzeżeń oraz uzyskaliśmy niezbędne informacje do przygotowania oferty.

Oświadczamy, że Istotne postanowienia umowy – stanowiące **Załącznik Nr 7** do niniejszej SIWZ zostały przez nas zaakceptowane i zobowiązujemy się w przypadku wyboru naszej oferty

do zawarcia umowy na podanych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

Oświadczamy, że wniesione wadium w formie pieniężnej prosimy zwrócić na numer rachunku bankowego w banku

(wypełniają Wykonawcy, którzy wnieśli wadium w formie pieniężnej)

Akceptujemy warunki płatności określone przez Zamawiającego w Istotnych postanowieniach umowy.

Zamówienia zrealizujemy sami/ przy udziale Podwykonawców* *

(* niepotrzebne skreślić)*

Podwykonawcom zostaną powierzone do wykonania następujące zakresy zamówienia (o ile jest znany): Zakres:

Nazwa podwykonawcy (jeżeli jest znany)

Wszelką korespondencję w sprawie niniejszego postępowania należy kierować do:

Imię i Nazwisko

Adres:

Telefon/Faks:

Adres e-mail:

Wzór podpisu i parafy osoby/osób podpisującej ofertę (Wykonawcy lub uprawnionego do reprezentacji wykonawcy):

Czytelne imię i nazwisko		Podpis	Parafa

Czy wykonawca jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem*? **tak/nie**
(niepotrzebne skreślić)

(*Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.

Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.

Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.)

Załącznikami do niniejszego Formularza Ofertowego są:

-
-
-

(Jeżeli dotyczy) Oświadczam, iż wraz z ofertą zostały złożone następujące dokumenty, które niniejszym wskazujemy (w trybie §10 ust. 2 rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy) w celu dokonania

przez Zamawiającego badania w zakresie spełniania przez Wykonawcę warunków udziału w postępowaniu i niepodleganiu wykluczeniu oraz, że oferowane urządzenie spełnia wymagania SIWZ:

-
-
-

Ofertę niniejszą składamy na¹ kolejno zaparafowanych i ponumerowanych stronach.

.....
(miejscowość, data)

.....
(podpis i pieczęć Wykonawcy)

¹ Należy wpisać łączną ilość stron, tj. formularz oferty wraz ze wszystkimi załącznikami i dokumentami wymaganymi w SIWZ.

.....
Nazwa i adres Wykonawcy
(pieczęć)

**WYKAZ WYKONANYCH ZAMÓWIEŃ
(BBA-2.262.15.2019)**

Wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych zamówień w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, **potwierdzający spełnianie przez Wykonawcę warunku posiadania niezbędnej wiedzy i doświadczenia postawionego w pkt 1.2.1.1 lit. A Części II SIWZ.** Podana wartość musi dotyczyć jednego zamówienia (przez co rozumie się, że musi wynikać z jednostkowej umowy zawartej z jednym podmiotem). Do wykazu należy dołączyć dowody potwierdzające, czy zamówienia te zostały wykonane lub są wykonywane należycie. Dokumenty muszą być wystawione przez zamawiającego/odbiorcę zamówienia.

Lp.	Nazwa i adres Zamawiającego/ odbiorcy	Przedmiot zamówienia (należy zamieścić informację pozwalającą na jednoznaczne stwierdzenie spełniania warunków udziału)	Wartość brutto	Termin wykonywania zamówienia (dzień- miesiąc- rok)	Sposób dysponowania (zasób własny/zasób podmiotu trzeciego)
1.					Zasób własny / zasób podmiotu trzeciego *
2.					Zasób własny / zasób podmiotu trzeciego *

Do wykazu załączono egzemplarz(e/y) dokumentów potwierdzających, że zamówienia te zostały wykonane należycie

.....
(miejscowość, data)

.....
(pieczęć i podpis Wykonawcy)

Istotne postanowienia umowy

w dniu 2019 r. w Warszawie pomiędzy:

Urzędem Ochrony Konkurencji i Konsumentów z siedzibą przy pl. Powstańców Warszawy 1, 00-950 Warszawa, posiadającym NIP PL 526-10-09-497, REGON 006212789, reprezentowanym przez:

Macieja Jabłońskiego - Dyrektora Generalnego Urzędu,

zwanym dalej „Zamawiającym”,

a

..... z siedzibą przy....., wpisaną do, posiadającą NIP, REGON, reprezentowaną przez :

.....,

zwaną dalej Wykonawcą,

w wyniku rozstrzygnięcia przez Zamawiającego procedury udzielenia zamówienia publicznego w trybie przetargu nieograniczonego, określonego w art. 39 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz.U. z 2018 r. poz. 1986 ze zm.), została zawarta umowa o następującej treści:

§ 1

1. Przedmiotem zamówienia jest zakup i wymiana urządzeń firmy FortiNet wchodzących w skład infrastruktury sieciowej i bezpieczeństwa Zamawiającego oraz zakup oprogramowania do zarządzania i analizy wymienionymi urządzeniami w Urzędzie Ochrony Konkurencji i Konsumentów (Plac Powstańców Warszawy 1, Warszawa) wraz z usługą wymiany i konfiguracji.
2. Szczegółowy opis i zakres przedmiotu umowy zawarty jest w Załączniku Nr 1 do niniejszej umowy stanowiący Szczegółowy Opis Przedmiotu Zamówienia oraz w Załączniku Nr 2, stanowiącym ofertę Wykonawcy.
3. Strony ustalają, iż realizacja przedmiotu umowy nastąpi w terminie do 30 dni od dnia podpisania umowy.
4. Dostarczone licencje/sublicencje oprogramowania będą uprawniać Zamawiającego do pobierania poprawek, aktualizacji i nowych wersji Oprogramowania przez cały okres gwarancji zadeklarowany przez Wykonawcę w Formularzu Ofertowym stanowiącym Załącznik nr 2 do Umowy, w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego Oprogramowania zgodnie z celem umowy.
5. Przez pojęcie „licencja/sublicencja” Zamawiający rozumie prawo do legalnego korzystania z oprogramowania do zarządzania i analizy urządzeń oraz innego dostarczonego oprogramowania, o którym mowa w § 1 ust. 1, na warunkach wskazanych przez producenta tego Systemu oraz na warunkach wskazanych w umowie.
6. Przez Oprogramowanie należy rozumieć w szczególności kompleksowe rozwiązanie informatyczne do konfigurowania, monitorowania i kompleksowego zarządzania urządzeniami, dostarczonymi w ramach i zgodnie z umową oraz inne oprogramowanie dostarczone wraz z urządzeniami zapory sieciowej.

§ 2

1. Wykonawca zobowiązuje się wykonać umowę zgodnie z obowiązującymi przepisami, treścią i jej celem, przy zachowaniu najwyższej staranności, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej i stosowanymi normami technicznymi, dobrymi praktykami i regułami.
2. Wykonawca ponosi pełną odpowiedzialność za wykonanie przedmiotu umowy.
3. W celu umożliwienia Wykonawcy wywiązania się ze swoich zobowiązań, Zamawiający zobowiązuje się w zakresie wymaganym dla prawidłowej realizacji umowy:
 - 1) współdziałać z Wykonawcą przy wykonywaniu umowy,
 - 2) zgłaszać Wykonawcy problemy związane z realizacją przedmiotu umowy.
4. Wykonawca oświadcza i gwarantuje, iż:
 - 1) posiada wiedzę, doświadczenie, urządzenia i narzędzia, w tym informatyczne niezbędne do prawidłowego wykonania umowy,
 - 2) personel Wykonawcy wykonujący prace w ramach realizacji umowy posiada doświadczenie i kwalifikacje niezbędne do prawidłowego wykonania umowy.
5. Wykonawca zobowiązuje się w szczególności:
 - 1) działać jedynie w zakresie swoich uprawnień i przestrzegać wskazówek Zamawiającego,
 - 2) do przestrzegania obowiązujących przepisów o ochronie danych osobowych oraz ochronie informacji prawnie chronionych,
 - 3) do odtworzenia utraconych, uszkodzonych lub zmienionych, w wyniku działania Wykonawcy danych i programów,
 - 4) do delegowania dedykowanego zespołu osób do realizacji umowy,
 - 5) do wykonania umowy w sposób niepowodujący zaprzestania lub zakłócenia pracy Zamawiającego,
 - 6) udostępniać na każde żądanie Zamawiającego dokumentację związaną z realizacją przedmiotu umowy.

§ 3

1. Wykonawca oświadcza i gwarantuje, że:
 - 1) dysponuje odpowiednią wiedzą, doświadczeniem i personelem niezbędnym do należytego wykonania zobowiązań wynikających z niniejszej umowy,
 - 2) wykona przedmiot umowy zgodnie z obowiązującymi przepisami i normami, w sposób profesjonalny, z uwzględnieniem najlepszych praktyk.
2. Wykonawca zobowiązuje się do zapewnienia we własnym zakresie i w ramach wynagrodzenia, o którym mowa w § 5 ust. 1 umowy wszystkich ewentualnych pozwoleń, zgód, certyfikatów wymaganych przez obowiązujące przepisy prawa w zakresie niezbędnym do prawidłowej realizacji umowy na czas nieokreślony.
3. Wykonawca zapewnia, że w wyniku zawarcia umowy nie dojdzie do naruszenia praw osób trzecich. W przypadku zgłoszenia wobec Zamawiającego roszczeń o naruszenie praw osób trzecich, Wykonawca podejmie na swój koszt wszelkie środki obrony Zamawiającego przed takimi roszczeniami lub zarzutami i spowoduje, że Zamawiający będzie od nich zwolniony, a także pokryje wszelkie koszty i straty, jakie poniesie Zamawiający z tego tytułu.
4. Urządzenia i oprogramowanie będące przedmiotem umowy muszą być fabrycznie nowe i odpowiadać co do jakości wymogom wyrobów dopuszczonych do obrotu na obszarze Unii Europejskiej oraz wymaganiom SIWZ.
5. Na sprzęt Wykonawca obowiązany jest posiadać w szczególności certyfikaty CE, zgodnie z obowiązującymi przepisami.

6. Wykonawca jest uprawniony do powierzenia wykonania umowy podwykonawcom, z zastrzeżeniem poniższych postanowień.
7. Wykonawca jest odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i jego pracowników w takim samym stopniu, jakby to były uchybienia lub zaniedbania jego własnych pracowników.
8. Wykonawca ponosi wyłączną odpowiedzialność za zapłatę wynagrodzenia podwykonawcom.
9. Wykonawca wykona przedmiot umowy przy udziale następujących podwykonawców:
 - 1) (wskazanie firmy, danych kontaktowych, osób reprezentujących podwykonawcę)- w zakresie..... (jeżeli dotyczy).
10. Wykonawca zobowiązany jest do poinformowania Zamawiającego w formie pisemnej o każdej zmianie danych dotyczących podwykonawców, jak również o ewentualnych nowych podwykonawcach, którym zamierza powierzyć prace w ramach realizacji umowy w terminie jednego dnia roboczego od dokonania zmiany.

§ 4

1. Wykonawca w ramach przysługującego mu wynagrodzenia, o którym mowa w § 5 ust. 1 umowy dostarczy Zamawiającemu przedmiot umowy na własny koszt i ryzyko.
2. Wydanie i odbiór przedmiotu umowy nastąpi po przeprowadzeniu odbioru ilościowego i jakościowego przedmiotu umowy, określonego w § 1 umowy.
3. Potwierdzeniem odbioru przedmiotu umowy będzie podpisany bez zastrzeżeń przez obie Strony Protokół odbioru, którego wzór stanowi Załącznik Nr 3 do umowy.
4. Wykonawca zawiadomi Zamawiającego o terminie dostawy przedmiotu umowy najpóźniej na 24 godziny przed planowanym terminem dostawy.
5. Odbiór przedmiotu umowy nastąpi w dni robocze, w godzinach pracy Zamawiającego, tj. od godz. 8.15 do godz. 16.15, w siedzibie Zamawiającego lub w inny sposób ustalony i zaakceptowany uprzednio przez obie Strony.
6. Wykonawca musi zapewnić, aby wszystkie czynności odbiorcze przedmiotu umowy w tym również podpisanie Protokołu odbioru, zostały zakończone w terminie określonym w § 1 ust. 3 umowy.
7. Do zaoferowanego Oprogramowania Wykonawca zobowiązuje się dostarczyć Zamawiającemu do jego siedziby: nośnik z wersją instalacyjną Oprogramowania (dla oprogramowania w wersji box), dane dostępowe do pobrania Systemu (w przypadku Systemu w formie elektronicznej lub objętego subskrypcją), licencje/sublicencje (umowy licencyjne w wersji papierowej lub elektronicznej w języku polskim lub angielskim) oraz wszystkie wymagane klucze licencyjne i aktywacyjne, instrukcje obsługi. W przypadku dostarczania licencji w formie elektronicznej należy je przesłać na adres:@uokik.gov.pl. W przypadku rejestracji Systemu drogą elektroniczną przez Wykonawcę należy użyć adresu poczty elektronicznej:@uokik.gov.pl oraz danych adresowych Zamawiającego jeśli takowe będą wymagane.
8. W przypadku gdy Zamawiający stwierdzi, że dostarczone licencje/sublicencje nie pozwalają na korzystanie z Oprogramowania, zgodnie z umową i ogólnymi warunkami Producenta (w tym również ze względu na wady nośnika, na którym zostały przekazane), lub Wykonawca nie dostarczy ogólnych warunków Producenta, Zamawiający odmówi podpisania Protokołu odbioru, a Wykonawca ponownie dostarczy nośniki Oprogramowania wraz z Dokumentacją, Licencją oraz ogólnymi warunkami na swój koszt i ryzyko w terminie 4 dni roboczych, licząc od daty otrzymania od Zamawiającego zawiadomienia o stwierdzonej nieprawidłowości.

9. Z chwilą podpisania przez Zamawiającego bez zastrzeżeń Protokołu odbioru, na Zamawiającego przechodzi prawo własności do przekazanego egzemplarza dokumentacji oraz do nośnika, na którym zostało utrwalone Oprogramowanie.

§ 5

1. Za wykonanie przedmiotu umowy określonego w § 1 Wykonawca otrzyma od Zamawiającego wynagrodzenie w kwocie brutto zł (słownie złotych:).
2. Wynagrodzenie, o którym mowa w ust. 1, obejmuje wszystkie koszty związane z realizacją przedmiotu umowy, niezbędne do wykonania przedmiotu umowy, w tym wynagrodzenie za przeniesienie autorskich praw majątkowych oraz prawa zezwalania na wykonywanie praw zależnych do utworów, wynagrodzenie za udzielenie licencji na zasadach określonych w umowie. Wynagrodzenie określone w ust. 1 wyczerpuje wszelkie roszczenia finansowe Wykonawcy z tytułu realizacji umowy.
3. Wypłata wynagrodzenia określonego w ust. 1, nastąpi w terminie do 21 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT, przelewem na rachunek bankowy wskazany przez Wykonawcę na fakturze VAT.
4. Podstawą do wystawienia faktury VAT będzie podpisany przez strony protokół odbioru potwierdzający prawidłowość wykonania przedmiotu umowy, o którym mowa w § 4 ust. 3 umowy.

§ 6

1. Wykonawca oświadcza i gwarantuje, że jakiegokolwiek utwory w rozumieniu art. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, zwanej „ustawą”, przekazane Zamawiającemu w trakcie realizacji umowy, ani korzystanie z nich przez Zamawiającego lub inne podmioty zgodnie z umową, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów ani praw do baz danych.
2. Wykonawca oświadcza, że posiada uprawnienia niezbędne do korzystania z utworów przekazanych Zamawiającemu w trakcie realizacji umowy.
3. Wykonawca oświadcza i gwarantuje, że licencje oraz inne utwory przekazane Zamawiającemu w trakcie realizacji umowy, ani korzystanie z nich przez Zamawiającego lub inne osoby zgodnie z umową nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów ani praw do baz danych.
4. Wykonawca oświadcza i gwarantuje, iż w ramach wynagrodzenia wskazanego w § 5 ust. 1 umowy z chwilą podpisania przez Strony protokołu odbioru udzielone zostają przez producenta Oprogramowania lub podmiot przez niego upoważniony bezterminowe, niewyłączne, rozciągające się na całe terytorium Rzeczypospolitej Polskiej, licencje na korzystanie z Oprogramowania, w szczególności na następujących polach eksploatacji:
 - 1) wprowadzenie i zapisywanie do pamięci komputera;
 - 2) odtwarzanie;
 - 3) przechowywanie;
 - 4) wyświetlanie;
 - 5) przystosowywanie;
 - 6) instalowanie i deinstalowanie Systemu pod warunkiem zachowania udzielonych licencji;
 - 7) korzystanie na wszystkich polach funkcjonalności;
 - 8) korzystanie i modyfikowanie dokumentów oraz danych wykorzystywanych przy pomocy Systemu.
5. Wykonawca dostarcza licencje Oprogramowania wraz z dokumentacją producenta niezbędną do korzystania z Oprogramowania.

6. Dostarczone Licencje muszą być wystawione na Zamawiającego.
7. Licencje, o których mowa w umowie udzielone zostaną na warunkach producenta Oprogramowania, o ile umowa nie stanowi inaczej.
8. Dostarczone przez Wykonawcę licencje muszą zapewniać pełną i prawidłową realizację celu umowy, zamierzonego przez Zamawiającego.
9. Wykonawca oświadcza i gwarantuje, że jeżeli nie jest producentem Oprogramowania, to uzyskał zgodę producenta lub podmiotu upoważnionego przez producenta na korzystanie z Oprogramowania na zasadach określonych w umowie, w tym na przekazywanie dokumentów zawierających warunki licencji.
10. Wykonawca oświadcza i gwarantuje, że licencje na Oprogramowanie nie zostaną wypowiedziane, za wyjątkiem istotnego naruszenia przez Zamawiającego warunków licencji. W przypadku wypowiedzenia licencji na Oprogramowanie pomimo braku istotnego naruszenia warunków licencji przez Zamawiającego, Wykonawca odpowiadać będzie za wynikłą z tego tytułu szkodę oraz w ramach wynagrodzenia, o którym mowa w § 5 ust. 1 umowy dostarczy odpowiednie licencje odpowiadające warunkom zawartym w umowie i Załączniku Nr 1 do umowy.
11. Z chwilą udzielenia licencji na Oprogramowanie własność nośników, na których je utrwalono przechodzi na Zamawiającego.
12. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z Oprogramowaniem, w tym zarzucających naruszenie praw własności intelektualnej, Wykonawca podejmie wszelkie działania mające na celu zażegnanie sporu i będzie zobowiązany naprawić każdą szkodę, za którą Zamawiający może stać się odpowiedzialny, lub do której naprawienia może zostać Zamawiający zobowiązany oraz ponieść w związku z tym wszelkie koszty, w tym koszty zastępstwa procesowego od chwili zgłoszenia roszczenia oraz koszty odszkodowań.
13. W przypadku wystąpienia osób trzecich wobec Zamawiającego z roszczeniami opartymi na twierdzeniu, iż używane przez Zamawiającego Oprogramowanie nie jest produktem wykonanym przez Producenta, Zamawiającemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub każde z osobna):
 - 1) prawo odstąpienia od umowy z wyłączeniem zapłaty na rzecz Wykonawcy jakichkolwiek kosztów, wynagrodzeń, odszkodowań itp.,
 - 2) zapłaty przez Wykonawcę na rzecz Zamawiającego kary umownej w wysokości 20% łącznej kwoty wynagrodzenia brutto określonego w § 5 ust. 1 umowy,
 - 3) prawo żądania odszkodowania uzupełniającego na zasadach ogólnych KC.

§ 7

1. Osobami sprawującymi nadzór nad realizacją umowy oraz upoważnionymi do podpisywania protokołów odbioru ze strony Zamawiającego są:, tel., e-mail, ze strony Wykonawcy są:, tel., e-mail
2. Osoby wymienione w ust. 1 odpowiedzialne są merytorycznie za nadzór nad prawidłowością i terminowością realizacji umowy, w szczególności upoważnione są do monitorowania należytego wykonania umowy oraz podpisania Protokołu odbioru.
3. Zmiana osób wskazanych w ust. 1 oraz ich danych kontaktowych nie wymaga zmiany umowy, a jedynie poinformowania drugiej Strony w formie pisemnej. Zawiadomienie takie powinno zostać podpisane przez osoby uprawnione do reprezentacji Stron.

§ 8

1. Wykonawca zapewni prawidłowe i sprawne działanie wdrożonej, nowej infrastruktury sieciowej i bezpieczeństwa Zamawiającego jako całości, jak również każdego z elementów tej infrastruktury oddzielnie (urządzeń i oprogramowanie) i udzieli 12 miesięcy gwarancji na infrastrukturę i wszystkie jej elementy (zgodnie z oświadczeniem Wykonawcy zawartym w Formularzu Ofertowym).
2. Wykonawca zapewni również wsparcie serwisowe dla urządzeń i oprogramowania, które będzie świadczone przez producenta lub autoryzowanego partnera serwisowego producenta, w ramach wynagrodzenia przysługującego Wykonawcy na podstawie niniejszej umowy na okres 12 miesięcy (zgodnie z udzieloną gwarancją) z możliwością jego odnawiania po tym czasie.
3. Zgłoszenia dotyczące wystąpienia wad, awarii mogą być przyjmowane pisemnie, telefonicznie, lub za pomocą poczty elektronicznej: adres producenta:, nr tel.:, adres e-mail:
4. W okresie gwarancji (zgodnie z terminem wskazanym w Formularzu Ofertowym), Wykonawca jest zobowiązany w ramach przysługującego mu na podstawie niniejszej umowy wynagrodzenia, do wspierania wdrożonej instalacji, co obejmuje również jej aktualizację na następujących zasadach:
 - 1) konsultacje techniczne (telefoniczne lub mailowe typu hot-line) dostępne ... dni w tygodniu, przez ... godzin dziennie (zgodnie z formularzem ofertowym);
 - 2) czas reakcji 4h licząc od momentu zgłoszenia wady;
 - 3) usunięcie wad nastąpi:
 - a) w odniesieniu do urządzeń sieciowych – na następny dzień roboczy, licząc od momentu zgłoszenia wady z wyłączeniem dni ustawowo wolnych od pracy,
 - b) w przypadku, gdy naprawa nie może być wykonana w czasie określonym w niniejszym paragrafie, z przyczyn niezależnych od Wykonawcy, Wykonawca dostarczy niezwłocznie sprzęt zastępczy o parametrach nie gorszych niż niesprawny sprzęt, a naprawy dokona w czasie do 7 dni roboczych od zgłoszenia wady,
 - c) w odniesieniu do oprogramowania – na następny dzień roboczy, licząc od momentu zgłoszenia wady z wyłączeniem dni ustawowo wolnych od pracy;
5. Dopuszczalne jest zastosowanie w ciągu 24 godzin od chwili zgłoszenia awarii rozwiązań zastępczych, przywracających utraconą funkcjonalność bez dokonania właściwej naprawy uszkodzonego elementu wdrożonego systemu. W takim przypadku czas naprawy i przywrócenia pełnej funkcjonalności nie może być dłuższy niż 14 dni kalendarzowych, licząc od momentu zgłoszenia wady.
6. Przyjmuje się, że Zamawiający zgłosił wadę skutecznie, jeżeli wysłał jej skrócony opis i wezwanie do jej usunięcia do Wykonawcy pocztą elektroniczną (na adres wskazany przez Wykonawcę). Wykonawca zobowiązuje się do zwrotnego potwierdzenia przyjęcia zgłoszenia wady.
7. Zgłaszanie wad musi być możliwe w trybie ... godziny x ... dni w tygodniu.
8. Bieg terminu gwarancji rozpoczyna się od daty odbioru końcowego.
9. W okresie gwarancji Wykonawca zobowiązuje się do bezpłatnego usunięcia stwierdzonych wad.
10. Gwarancja obejmuje wszelkie wady z wyjątkiem uszkodzeń mechanicznych, wad spowodowanych niewłaściwym lub niezgodnym z instrukcją obsługą użytkowaniem produktu oraz wad spowodowanych zdarzeniami losowymi.

11. Jeżeli usunięcie ujawnionej wady wdrożonego oprogramowania lub urządzeń jest możliwe wyłącznie w drodze dokonania zakupu jakichkolwiek udoskonaleń (w tym: unowocześnień, upgrad'ów, dodatków sprzętowych, wszelkiego rodzaju usług, serwisów, licencji i uprawnień), Wykonawca jest zobowiązany dokonać tego zakupu na własny koszt i zainstalować przedmiot zakupu we wdrożonej infrastrukturze sieciowej i bezpieczeństwa Zamawiającego.
12. Wykonawca pokrywa w ramach gwarancji wszelkie koszty napraw i wymiany elementów oprogramowania lub urządzeń, w tym koszty dojazdu, transportu, demontażu, montażu, odinstalowania lub zainstalowania.
13. Udzielona przez Wykonawcę gwarancja nie wyłącza uprawnień Zamawiającego wynikających z rękojmi za wady oraz uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producenta przełączników lub urządzeń.
14. Wszelkie naprawy gwarancyjne jak i serwisowanie infrastruktury muszą odbywać się w siedzibie Zamawiającego. Zakres gwarancji określony będzie w kartach gwarancyjnych i innych dokumentach, które Wykonawca powinien dostarczyć najpóźniej w dniu podpisania protokołu odbioru przedmiotu zamówienia.
15. Okres gwarancji lub rękojmi ulega odpowiedniemu przedłużeniu o czas, w ciągu którego, wskutek wady przedmiotu umowy objętego gwarancją, Zamawiający nie mógł z niego korzystać.
16. Wykonawca do urządzeń dostarczonych Zamawiającemu na podstawie umowy dołącza karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji.

§ 9

1. Wykonawca jest zobowiązany do zachowania w tajemnicy przed osobami trzecimi wszelkich informacji o Zamawiającym oraz informacji, do których uzyskał dostęp w związku z wykonywaniem umowy.
2. Z obowiązku, o którym mowa w ust. 1, zwalnia Wykonawcę jedynie pisemna zgoda Zamawiającego.
3. Obowiązek, o którym mowa w ust. 1, nie dotyczy informacji dostępnych publicznie oraz informacji żądanych przez uprawnione organy, w zakresie, w jakim są one uprawnione do ich żądania zgodnie z obowiązującymi przepisami prawa.

§ 10

1. Zamawiający naliczy Wykonawcy karę umowną za niedotrzymanie terminu realizacji umowy, określonego w § 1 ust. 3, w wysokości 0,4 % wynagrodzenia brutto, określonego w § 5 ust. 1 za każdy rozpoczęty dzień zwłoki.
2. Zamawiający naliczy Wykonawcy karę umowną za opóźnienie w usunięciu wad powodujących niemożność korzystania z oprogramowania i urządzeń stwierdzonych przy odbiorze lub w okresie gwarancji, w wysokości 0,3 % wynagrodzenia brutto, określonego w § 5 ust. 1 za każdy rozpoczęty dzień zwłoki, liczonej od końcowych terminów określonych w § 8 ust. 4 pkt 3.
3. Zamawiający naliczy Wykonawcy karę umowną za opóźnienie w usunięciu w okresie gwarancji pozostałych wad, w wysokości 0,1 % wynagrodzenia brutto, określonego w § 5 ust. 1 za każdy rozpoczęty dzień zwłoki, liczonej od końcowych terminów określonych w § 8 ust. 4 pkt 3.
4. W przypadku, gdy zwłoka w realizacji przedmiotu umowy w zakresie określonym w §1 ust 1 przekroczy 8 dni, Zamawiający ma prawo odstąpić od umowy w niezrealizowanym zakresie, a Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15 % wynagrodzenia brutto, określonego w § 5 ust. 1 niniejszej umowy.
5. Zamawiający może odstąpić od umowy w niezrealizowanym zakresie w trybie natychmiastowym, w przypadku nieprzestrzegania przez Wykonawcę któregośkolwiek z warunków niniejszej umowy,

przy czym odstąpienie od umowy musi być poprzedzone wezwaniem Wykonawcy do realizacji przedmiotu umowy zgodnie z opisem przedmiotu zamówienia oraz postanowieniami umowy.

6. Zamawiający naliczy Wykonawcy karę umowną z tytułu odstąpienia od umowy lub wypowiedzenia umowy z przyczyn leżących po stronie Wykonawcy w wysokości 15 % wynagrodzenia brutto, określonego w § 5 ust. 1 niniejszej umowy.
7. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przewyższającego wartość zastrzeżonych kar umownych, na zasadach ogólnych.
8. Wykonawca wyraża zgodę na potrącenie ewentualnych kar umownych z wynagrodzenia przysługującego za wykonanie przedmiotu umowy.
9. Zamawiający może odstąpić od nałożenia kary lub ją obniżyć, jeżeli Wykonawca wykaże, że opóźnienie nastąpiło z przyczyn całkowicie od niego niezależnych, których nie mógł przewidzieć i którym nie mógł zapobiec.
10. Zapłata przez Wykonawcę kar umownych z tytułu niewykonania lub nienależytego wykonania umowy, nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego ustalone kary umowne na zasadach ogólnych, przy czym odpowiedzialność Wykonawcy z tytułu kar umownych ograniczona jest do 100% wartości umowy brutto, o której mowa w § 5 ust. 1 umowy.

§ 11

1. Zamawiający może wypowiedzieć, rozwiązać lub odstąpić od części lub całości umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. Zamawiający może odstąpić od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy. W tym przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu należytego wykonania części umowy.
3. Zamawiający może rozwiązać umowę w całości lub w części w terminie 14 dni w następujących przypadkach:
 - 1) otwarcia postępowania likwidacyjnego Wykonawcy;
 - 2) wykreślenia Wykonawcy z właściwej ewidencji;
 - 3) zajęcia majątku Wykonawcy w stopniu uniemożliwiającym mu należyte wykonanie umowy;
 - 4) utraty praw do wykonywania prac w zakresie wdrożenia lub prac rozwojowych (np. utrata autoryzacji producenta licencji Systemu przez Wykonawcę).
4. W przypadku rozwiązania umowy przez Zamawiającego, w sytuacjach, o których mowa w ust. 3 niniejszego paragrafu:
 - 1) strony zobowiązują się w terminie 14 dni od dnia odstąpienia od umowy do sporządzenia protokołu, który będzie stwierdzał stan realizacji przedmiotu umowy do dnia odstąpienia od umowy;
 - 2) wysokość wynagrodzenia należna Wykonawcy zostanie ustalona proporcjonalnie na podstawie stwierdzonego protokołem zakresu należycie wykonanego przedmiotu umowy zaakceptowanego przez Zamawiającego bez zastrzeżeń, o ile wykonany zakres przedmiotu umowy będzie miał dla Zamawiającego znaczenie;
 - 3) Strony dokonują rozliczenia prawidłowo wykonanych prac do dnia rozwiązania lub odstąpienia od umowy w oparciu o odpowiednie stosowanie postanowień umowy w szczególności w zakresie procedur odbioru, podstaw wystawiania faktur, zasad i terminów płatności.

§ 12

1. W każdym wypadku Strona nie jest odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań wynikających z umowy, jeżeli udowodni, iż niewykonanie lub nienależyte wykonanie zostało spowodowane wystąpieniem siły wyższej tj. zdarzeń zewnętrznych, na które Strony nie mają wpływu, a które uniemożliwiają wykonanie zobowiązań wynikających z niniejszej Umowy, których nie można było przewidzieć i których nie dało się uniknąć nawet w przypadku dołożenia przez Strony najwyższej staranności, a w szczególności:
 - 1) wojna, w tym wojna domowa, zamieszki, rozruchy i akty terroryzmu;
 - 2) katastrofy naturalne, takie jak huragany, trzęsienia ziemi, powodzie;
 - 3) wybuchy, pożary;
 - 4) przerwy w dostawie prądu trwające jednorazowo nieprzerwanie co najmniej 3 dni robocze.
2. Strona dotknięta działaniem siły wyższej poinformuje pisemnie drugą Stronę o wystąpieniu siły wyższej oraz o przewidywanych konsekwencjach w wykonaniu zobowiązań przewidzianych w niniejszej Umowie w celu wspólnego ustalenia dalszego postępowania, w ciągu 3 dni roboczych od wystąpienia zdarzenia siły wyższej.
3. W razie zaistnienia okoliczności siły wyższej terminy realizacji umowy przedłużają się o okres jej trwania.

§ 13

1. Wszelkie zmiany i uzupełnienia niniejszej umowy wymagają formy pisemnej pod rygorem nieważności i zgody obu Stron.
2. Zamawiający przewiduje możliwość zmian postanowień niniejszej umowy w przypadkach, gdy:
 - 1) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu umowy, chyba że zmiana taka znana była w chwili składania oferty;
 - 2) nastąpi zmiana założeń strategicznych Zamawiającego, które w istotny sposób wpływają na sposób realizacji przedmiotu umowy. Za istotny sposób uważa się rzeczywistą, obiektywną potrzebę zmiany celów wynikającą z potrzeb Zamawiającego której nie przewidywano w ramach Opisu przedmiotu zamówienia określonego w Załączniku Nr 1 do umowy w chwili podpisania umowy;
 - 3) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest konieczna w celu prawidłowego wykonania przedmiotu umowy, w szczególności gdy konieczność zmiany została ujawniona na etapie prac analitycznych i projektowych i wymaga zmiany:
 - a. wynikających z przyczyn technicznych;
 - b. sposobu wykonania umowy w obszarach: organizacyjnym, wykorzystywanych narzędzi, przyjętych metod i kanałów komunikacji;
 - 4) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili podpisania umowy. Jako korzystniejsze dla Zamawiającego należy traktować rozwiązania odpowiadające Wymaganiom Zamawiającego w większym stopniu z punktu widzenia kosztów utrzymania, wydajności infrastruktury lub wyższej użyteczności;
 - 5) nastąpi zmiana stawki podatku od towarów i usług;

- 6) strony są uprawnione do wprowadzenia do umowy zmian nieistotnych, to jest innych, niż zmiany zdefiniowane w art. 144 ust. 1e ustawy Pzp oraz zmian wskazanych w art. 144 ust. 1 pkt. 2-6 ustawy Pzp.
5. Zmiany umowy w trybie aneksu do umowy nie wymagają w szczególności zmian nazw/określeń Stron, siedziby Stron, Załączników do umowy jak również osób odpowiedzialnych za realizację przedmiotu umowy ze strony Wykonawcy oraz przedstawicieli Zamawiającego.
6. Strony zobowiązane są do informowania się wzajemnie o okolicznościach uzasadniających konieczność dokonania zmiany umowy.

§ 14

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy powszechnie obowiązujące, w tym przepisy Kodeksu cywilnego oraz ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.
2. Wykonawca ma świadomość, iż umowa i dane go identyfikujące podlegają udostępnieniu na podstawie informacji o dostępie do informacji publicznej i stanowią informację publiczną w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.
3. Każda zmiana niniejszej umowy wymaga zachowania formy pisemnej pod rygorem nieważności.

§ 15

Spory mogące wyniknąć na tle realizacji niniejszej umowy będą rozstrzygane przez Sąd właściwy miejscowo dla siedziby Zamawiającego.

§ 16

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym egzemplarzu dla każdej ze Stron.

ZAMAWIAJĄCY

WYKONAWCA

Protokół odbioru

Sporządzony w dniu 2019 r.

Zakres wykonania zamówienia obejmował
.....
.....
.....

Zamówienie zostało wykonane zgodnie z umową nr BBA-2/022...-.../2019 z 2019 r.
zawartą pomiędzy

Urzędem Ochrony Konkurencji i Konsumentów

a

.....

Odbioru dokonali w imieniu:

ZAMAWIAJĄCEGO –

WYKONAWCY –

Uwagi i wnioski osób biorących udział w odbiorze **:

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

Niniejszy protokół stanowi podstawę do wystawienia faktury.

ZAMAWIAJĄCY

WYKONAWCA

* należy skreślić niepotrzebne

**w przypadku braku uwag należy wpisać „BRAK UWAG”

.....
(pieczęć adresowa firmy)

Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia

Wykaz winien potwierdzać spełnianie warunku dysponowania osobami zdolnymi do wykonania zamówienia, zgodnie z wymogami określonymi w pkt 1.2.1.2 lit. A Części II SIWZ.

(BBA-2.262.15.2019)

l.p.	Imię i nazwisko	Kwalifikacje zawodowe, uprawnienia, doświadczenia i wykształcenie (należy podać wszystkie informacje niezbędne do potwierdzenie spełniania przez pracownika postawionych warunków)	Zakres wykonywanych przez nich czynności	Informacja o podstawie do dysponowania osobami - Forma zatrudnienia (zasób własny/zasób podmiotu trzeciego*)
1				
2				

- *Niepotrzebne skreślić*
- W przypadku, jeśli Wykonawca zamierza polegać na zasobach (osobach zdolnych do wykonania zamówienia) innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków, Wykonawca zobowiązany jest wykazać Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawić w tym celu **pisemne** zobowiązanie tych podmiotów do oddania mu do dyspozycji osób zdolnych do realizacji zamówienia na okres korzystania z nich przy wykonywaniu zamówienia.

.....
(miejscowość, data)

.....
(podpis i pieczęć Wykonawcy)