AMW REWITA

AMW REWITA Sp. z o.o.

03-310 Warszawa, ul. św. J. Odrowąża 15

ZATWIERDZAM

PREZES ZARZĄDU Damian Pietrzyk

WICEPREZES ZARZĄDU Elżbieta Cendrzak

.....

Kierownik Zamawiającego

dnia 20/03/2018 r.

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

zwana dalej „SIWZ"

w postępowaniu o udzielenie zamówienia publicznego prowadzonego

w trybie przetargu nieograniczonego pn.

„Dostawa i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o."

Nr postępowania: RWT/PZP/9/2018

Wartość szacunkowa zamówienia **nie przekracza** kwoty określonych w przepisach wydanych na podstawie art. 11 ust. 8 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2015r. poz. 2164 ze zm.)zwanej w dalszej części specyfikacji „Pzp".

Zamawiający oczekuje, ze Wykonawcy zapoznają się dokładnie z treścią niniejszej SIWZ. Wykonawca ponosi ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów oraz przedłożenia oferty nie odpowiadającej wymaganiom Zamawiającego.

Departament Organizacyjny Zespół Zakupów Koordynator Dorota Osińska

Warszawa, marzec 2018 r.

DYREKTOR Departamentu Organizacyjnego AMW REWITA Sp. z o.o. Joanna Gomułka

Departament Organizacyjny Zespół Informatyczny Koordynator Rafał Lenarczyk

ul. Św. Jacka Odrowąża 15, 03-310 Warszawa, tel. +48 22 270-95-50, fax: + 48 22 270-21-43, e-mail: sekretariat@rewita.pl
NIP: 701-030-24-56, REGON: 142990254, KRS: 0000394569, Kapitał zakładowy 534 072 000,00 PLN wpłacony w całości
www.rewita.pl

AMW REWITA

Rozdział I. Nazwa (firma) oraz adres Zamawiającego.

AMW REWITA Sp. z o.o.
ul. św. J. Odrowąża 15
03-310 Warszawa

Telefon: 222709558
Adres e-mail: zp@rewita.pl,
Faks: 222702143
Strona internetowa: www.rewita.pl
Godziny pracy od 08:00 do 15:00, od poniedziałku do piątku
NIP: 7010302456, Regon:142990254

Numer postępowania, którego dotyczy niniejszy dokument oznaczone jest znakiem:

RWT/PZP/9/2018

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

Rozdział II. Tryb udzielenia zamówienia.

1. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 i nast. Pzp.
2. W zakresie nieuregulowanym niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ", zastosowanie mają przepisy Pzp.
3. Wartość zamówienia nie przekracza równowartości kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 Pzp.

Rozdział III. Opis przedmiotu zamówienia i wymagania Zamawiającego.

1. **Przedmiotem zamówienia jest dostawa i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o.**
2. Szczegółowy opis przedmiotu zamówienia znajduje się w **Załączniku nr 1 do SIWZ.**
3. Wspólny Słownik Zamówień CPV: 48000000-8 Pakiety oprogramowania i systemy informatyczne
4. Zamawiający nie dopuszcza składania ofert częściowych.
5. Zamawiający nie dopuszcza składania ofert wariantowych.
6. Zamawiający nie przewiduje zamówień, o których mowa w art. 67 ust. 1 pkt 6 Pzp.
7. Postępowanie nie jest prowadzone w celu zawarcia umowy ramowej.
8. Zamawiający nie przewiduje możliwości udzielania zaliczek.
9. Zamawiający nie przewiduje dogrywki elektronicznej.

10. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę prac związanych z realizacją dostaw.
11. Zamawiający nie wymaga zatrudnienia przez Wykonawcę lub Podwykonawcę na podstawie umowy o pracę osób wykonujących czynności w zakresie realizacji przedmiotowego zamówienia.
12. Zamawiający zastrzega, że dostarczony przedmiot zamówienia **musi spełniać wszystkie normy przewidziane przepisami prawa.**
13. Oferowany przedmiot zamówienia **musi być fabrycznie nowy**.
14. W przypadku, w którym Wykonawca korzysta w wykonaniu umowy z Podwykonawców lub podmiotów trzecich, na zasoby których powoływał się celem wykazania spełnienia warunków w postępowaniu o udzielenie zamówienia publicznego, zastosowanie znajduje reguła, że jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 Pzp, Wykonawca jest zobowiązany wykazać Zamawiającemu, iż proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia publicznego i uzyskać pisemną zgodę Zamawiającego na taką zmianę.
15. Przedmiot zamówienia obejmuje transport do miejsca przeznaczenia oraz instalację oraz wdrożenie w miejscu wskazanym przez Zamawiającego.
16. Dostawa – realizacja zamówienia nastąpi na koszt i ryzyko Wykonawcy.
17. Wykonawca zobowiązuje się dostarczyć przedmiot zamówienia zorganizowanym przez siebie transportem na koszt i ryzyko Wykonawcy. Zamawiający nie będzie ponosił odpowiedzialności za uszkodzenia powstałe podczas załadunku, transportu oraz rozładunku.
12. Zamawiający dopuszcza powierzenie części zamówienia podwykonawcom. W takim przypadku Wykonawca na podstawie art. 36b ust. 1 Pzp ma obowiązek wskazać w ofercie część zamówienia, którą zamierza powierzyć podwykonawcom. Brak takiego wskazania oznacza, że Wykonawca **nie będzie korzystał z podwykonawstwa przy realizacji zamówienia**. Zmiana podwykonawcy podczas realizacji umowy, możliwa będzie jedynie za pisemną zgodą Zamawiającego.

Rozdział IV. Termin wykonania zamówienia.

Zamawiający wymaga realizacji zamówienia w terminie **do 30 dni od dnia podpisania umowy.**

Rozdział V. Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków.

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

1) **nie podlegają wykluczeniu** – o udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą brak podstaw do wykluczenia z powodu niespełnienia warunków określonych w art. 24 ust 1 Pzp. Zamawiający uzna, że Wykonawca nie podlega wykluczeniu z postępowania, zgodnie z art. 24 ust. 1 Pzp, jeżeli z przedstawionych przez Wykonawcę oświadczeń i dokumentów wynikać będzie, że nie

występują uwarunkowania określone w art. 24 ust. 1 pkt 12-23 Pzp. W przypadkach, gdy Wykonawca wykazując spełnianie warunków, polega na zasobach innych podmiotów, w stosunku do żadnego z tych podmiotów nie mogą występować uwarunkowania art. 24 ust. 1 pkt 12-23 Pzp.

2) spełniają warunki udziału w postępowaniu, w zakresie:
   a) **kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów finansowej** – Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny.

   b) **sytuacji ekonomicznej lub finansowej** – Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny.

   c) **posiadania zdolności technicznej lub zawodowej** – Zamawiający wymaga na potwierdzenie spełnienia tego warunku w następujący sposób:
   Wykonawcy muszą:
   a) legitymować się doświadczeniem w zakresie wdrażania systemów bezpieczeństwa oraz systemów zarządzania i katalogowania usług IT w dużych rozproszonych organizacjach, polegającym na wykonaniu w ciągu ostatnich 3 lat prowadzenia działalności lub jeśli okres działalności jest krótszy – to w tym okresie, co najmniej:
   - dwóch dostaw zaoferowanego w ramach realizacji niniejszego postępowania urządzenia typu UTM/NGFW, o wartości co najmniej 45 000,00 zł brutto każda
   - dwóch dostaw zaoferowanego w ramach realizacji niniejszego postępowania modułu ochrony systemu pocztowego, o wartości co najmniej 30 000,00 zł brutto każda
   - dwóch dostaw zaoferowanego w ramach realizacji niniejszego postępowania oprogramowania do centralnego zarządzania infrastrukturą IT, obejmujących co najmniej 150 stacji każda.
   b) posiadać Certyfikat producenta wdrażanego rozwiązania;

2. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia w oparciu o treść art. 23 ustawy Pzp. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego:
   1) warunek określony w pkt. 1 ppkt 1) – winien spełniać każdy z Wykonawców samodzielnie;
   2) warunek określony w pkt. 1 ppkt. 2) lit. a) – winni spełniać ci członkowie konsorcjum, którzy będą faktycznie realizować część zamówienia, do której wykonania wymagane jest posiadanie uprawnień ustawowych;
   3) warunki określone w punktach: pkt. 1 ppkt. 2) lit. b) oraz pkt. 1 ppkt. 2) lit. c) – zostaną spełnione, jeżeli spełnia je samodzielnie, chociaż jeden z Wykonawców wspólnie ubiegających się o zamówienie (art. 23);
3. Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego;
4. Jeżeli oferta Wykonawców, o których mowa w art. 23 ust. 1, zostanie wybrana, zamawiający zastrzega możliwość żądania przed zawarciem umowy w sprawie zamówienia publicznego, przedłożenia umowy regulującej współpracę tych Wykonawców.
5. Zamawiający może, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych

zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze ze strony Wykonawcy może mieć negatywny wpływ na realizację zamówienia.

6. Wykonawca może, w celu potwierdzenia spełniania warunków, o których mowa w rozdz. V.1.2) lit. b) i c) niniejszej SIWZ, w stosownych sytuacjach, w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
7. Zamawiający jednocześnie informuje, iż „stosowna sytuacja" o której mowa w rozdziale V. 3 niniejszej SIWZ wystąpi wyłącznie w przypadku kiedy:
   1) Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów udowodni Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia;
   2) Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 i ust. 5 Pzp.

Rozdział VI. Podstawy wykluczenia, o których mowa w art. 24 ust. 5 ustawy Pzp.

Dodatkowo Zamawiający przewiduje wykluczenie Wykonawcy:

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 2015 r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615) 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 2015 r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016 r. poz. 615);
2) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności, gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
3) jeżeli Wykonawca lub osoby, o których mowa w art. 24 ust. 1 pkt 14 Pzp, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 Pzp z:
   a) Zamawiającym,
   b) osobami uprawnionymi do reprezentowania Zamawiającego,
   c) członkami komisji przetargowej,
   d) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a Pzp

– chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu;

4) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z Zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 Pzp, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;

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

Rozdział VII. Wykaz oświadczeń lub dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia.

1. Do oferty każdy Wykonawca musi dołączyć:

   1) aktualne na dzień składania ofert oświadczenie w zakresie wskazanym w **załączniku nr 3** do SIWZ. Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

   2) Wypełniony formularz ofertowy – **załącznik nr 2 do SIWZ.**

   3) Pełnomocnictwa do reprezentowania wykonawcy, w szczególności do podpisania oferty, dokumentów i oświadczeń, o ile przedstawiciel Wykonawcy działa na podstawie pełnomocnictwa.

2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie, o którym mowa w rozdziale VI. 1 niniejszej SIWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to ma potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia.

3. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o podwykonawcach w oświadczeniu, o którym mowa w rozdziale VII. 1 niniejszej SIWZ.

4. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia - w zakresie, w jakim powołuje się na ich zasoby - warunków udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w rozdziale VII. 1 niniejszej SIWZ.

5. **Zamawiający informuje, iż zgodnie z art. 24 aa ustawy, w pierwszej kolejności dokona oceny ofert a następnie zbada czy wykonawca, którego oferta została oceniona jako najkorzystniejsza według kryterium oceny ofert określonym w SIWZ, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.**

6. **Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:**

   a) Wykaz: co najmniej dwóch dostaw zaoferowanego w ramach realizacji niniejszego postępowania urządzenia typu UTM/NGFW, o wartości co najmniej 45 000,00 zł każda, co najmniej dwóch dostaw zaoferowanego w ramach realizacji niniejszego postępowania modułu ochrony systemu pocztowego, o wartości co najmniej 30 000,00 zł każda, co najmniej dwóch dostaw zaoferowanego w ramach realizacji niniejszego postępowania oprogramowania do centralnego zarządzania infrastrukturą IT, obejmujących co najmniej 150 stacji każda;

   b) odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy;

   c) oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności;

   d) oświadczenia wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne.

7. **Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 Pzp, przekaże Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 Pzp. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.**

8. W zakresie nieuregulowanym SIWZ, zastosowanie mają przepisy rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r., poz. 1126).
9. Jeżeli Wykonawca nie złoży oświadczenia, o którym mowa w rozdziale VII. 1. niniejszej SIWZ, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 Pzp, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia, poprawienia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.

AMW REWITA

Rozdział VIII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje Zamawiający oraz Wykonawcy mogą przekazywać pisemnie, faksem lub drogą elektroniczną, za wyjątkiem oferty, umowy oraz oświadczeń i dokumentów wymienionych w rozdziale VII niniejszej SIWZ (również w przypadku ich złożenia w wyniku wezwania o którym mowa w art. 26 ust. 3 Pzp) dla których dopuszczalna jest forma pisemna.
2. W korespondencji kierowanej do Zamawiającego Wykonawca winien posługiwać się numerem sprawy określonym w SIWZ, tj. **RWT/PZP/9/2018.**
3. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę pisemnie winny być składane na adres: **AMW REWITA Sp. z o.o., ul. św. J. Odrowąża 15, 03-310 Warszawa**
4. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę drogą elektroniczną winny być kierowane na adres: **zp@rewita.pl**
5. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje przekazane w formie elektronicznej wymagają na żądanie każdej ze stron, niezwłocznego potwierdzenia faktu ich otrzymania.
6. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ.
7. **Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert, Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o którym mowa powyżej, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.**

   Wyjaśnienie i zmiany treści SIWZ oraz wszelkie informacje dotyczące przedmiotowego postępowania zamieszczane będą wyłącznie na stronie internetowej Zamawiającego www.rewita.pl. Zamawiający zaleca śledzenie strony internetowej w celu uzyskania aktualnych informacji dotyczących przedmiotowego postępowania.
8. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w rozdziale VIII. 7 niniejszej SIWZ.
9. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
10. Zamawiający nie przewiduje zwołania zebrania Wykonawców.
11. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami jest:

    w sprawach proceduralnych : Pani Dorota Osińska e-mail: zp@rewita.pl

    w sprawach merytorycznych : Pan Rafał Lenarczyk e-mail: r.lenarczykl@rewita.pl

Jednocześnie Zamawiający informuje, że przepisy Pzp nie pozwalają na jakikolwiek inny kontakt - zarówno z Zamawiającym jak i osobami uprawnionymi do porozumiewania się z Wykonawcami - niż wskazany w niniejszym rozdziale SIWZ. Oznacza to, że Zamawiający nie będzie reagował na inne formy kontaktowania się z nim, w szczególności na kontakt telefoniczny lub/i osobisty w swojej siedzibie.

Rozdział IX. Wymagania dotyczące wadium.

1. Zamawiający nie wymaga wniesienia wadium.

Rozdział X. Termin związania ofertą.

1. Wykonawca będzie związany ofertą przez okres **30 dni.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy, samodzielnie lub na wniosek Zamawiającego, 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.
3. Odmowa wyrażenia zgody na przedłużenie terminu związania z ofertą nie powoduje utraty wadium.

Przedłużenie terminu związania z ofertą jest dopuszczalne tylko z jednoznacznym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe z wniesieniem nowego wadium na przedłużony okres związania z ofertą. Jeżeli przedłużenie terminu związania z ofertą dokonywane jest po wyborze oferty najkorzystniejszej obowiązek wniesienia nowego wadium lub jego przedłużenia dotyczy jedynie Wykonawcy, którego oferta została wybrana jako najkorzystniejsza.

Rozdział XI. Opis sposobu przygotowywania oferty.

1. Oferta musi zawierać następujące oświadczenia i dokumenty:
   1) wypełniony Formularz ofertowy sporządzony z wykorzystaniem wzoru stanowiącego Załącznik nr 2 do SIWZ, zawierający w szczególności: wskazanie oferowanego przedmiotu zamówienia, łączną cenę ofertową brutto, oświadczenie o okresie związania ofertą i o akceptacji wszystkich postanowień SIWZ, oraz wzoru umowy bez zastrzeżeń, a także informację którą część zamówienia Wykonawca zamierza powierzyć podwykonawcy;
   2) oświadczenia wymienione w rozdziale VII. 1-4 niniejszej SIWZ;
   3) Certyfikat producenta wdrażanego rozwiązania.
2. Oferta musi być napisana w języku polskim, na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką oraz podpisana przez osobę(y) upoważnioną do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty.
3. W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne pełnomocnictwo w oryginale lub kopii poświadczonej notarialnie.
4. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
5. Wykonawca ma prawo złożyć tylko jedną ofertę, zawierającą jedną, jednoznacznie opisaną propozycję. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
6. Treść złożonej oferty musi odpowiadać treści SIWZ.
7. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.

8. Zaleca się, aby każda zapisana strona oferty była ponumerowana kolejnymi numerami, a cała oferta wraz z załącznikami była w trwały sposób ze sobą połączona (np. zbindowana, zszyta uniemożliwiając jej samoistną dekompletację), oraz zawierała spis treści.
9. Poprawki lub zmiany (również przy użyciu korektora) w ofercie, powinny być parafowane własnoręcznie przez osobę podpisującą ofertę.
10. Ofertę należy złożyć w zamkniętej kopercie, w siedzibie Zamawiającego i oznakować w następujący sposób:

AMW REWITA Sp. z o.o.
ul. św. J. Odrowąża 15, 03-310 Warszawa
„ Oferta w postępowaniu na dostawę i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o."
Otworzyć na jawnym otwarciu ofert w dniu 28.03.2018 r. o godz. 11:00

i opatrzyć nazwą i dokładnym adresem Wykonawcy.

Konsekwencje złożenia oferty niezgodnie z ww opisem ponosi Wykonawca.

11. Zamawiający informuje, iż zgodnie z art. 8 w zw. z art. 96 ust. 3 Pzp oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępniane i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
12. 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. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
13. Zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji będzie traktowane, jako bezskuteczne i skutkować będzie zgodnie z uchwałą SN z 20 października 2005 (sygn. III CZP 74/05) ich odtajnieniem.
14. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 90 Pzp, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.
15. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone wg takich samych zasad, jak składana oferta tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA". Koperty oznaczone

„ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.

16. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia, według tych samych zasad jak wprowadzanie zmian i poprawek z napisem na kopercie „WYCOFANIE". Koperty oznakowane w ten sposób będą otwierane w pierwszej kolejności po potwierdzeniu poprawności postępowania Wykonawcy oraz zgodności ze złożonymi ofertami. Koperty ofert wycofywanych nie będą otwierane.
17. Do przeliczenia na PLN wartości wskazanej w dokumentach złożonych na potwierdzenie spełniania warunków udziału w postępowaniu, wyrażonej w walutach innych niż PLN, Zamawiający przyjmie średni kurs publikowany przez Narodowy Bank Polski z dnia wszczęcia postępowania.
18. Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 Pzp zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy PZP). Wszelkie niejasności i wątpliwości dotyczące treści zapisów w SIWZ należy zatem wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym w rozdziale VII niniejszej SIWZ. Przepisy Pzp nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.
19. Wszelkie błędne oznaczenia oferty (koperty) obciążają Wykonawcę, z tytułu których nie ma on prawa do żadnych roszczeń wobec Zamawiającego.

Rozdział XII. Miejsce oraz termin składania i otwarcia ofert.

1. Ofertę należy złożyć do dnia **28.03.2018 r.** do godz. **10:00** w siedzibie Zamawiającego tj. **AMW REWITA Sp. z o.o., ul. św J. Odrowąża 15, 03-310 Warszawa, sekretariat.**
2. Decydujące znaczenie dla oceny zachowania terminu składania ofert ma data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską.
3. Oferta złożona po terminie wskazanym w rozdz. XI. 1 niniejszej SIWZ zostanie zwrócona Wykonawcy zgodnie z zasadami określonymi w art. 84 ust. 2 ustawy PZP.
4. Otwarcie ofert nastąpi w siedzibie Zamawiającego – sala konferencyjna, w dniu **28.03.2018r.,** o godzinie **11:00.**
5. Otwarcie ofert jest jawne.
6. Podczas otwarcia ofert Zamawiający odczyta informacje, o których mowa w art. 86 ust. 4 ustawy PZP.
7. Niezwłocznie po otwarciu ofert zamawiający zamieści na stronie **www.rewita.pl** informacje dotyczące:
   a) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;
   b) firm oraz adresów Wykonawców, którzy złożyli oferty w terminie;
   c) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

AMW REWITA

Rozdział XIII. Opis sposobu obliczenia ceny.

1. Przez cenę ofertową należy rozumieć cenę w rozumieniu art. 3 ust. 1 pkt. 1 i ust. 2 ustawy z dnia 9 maja 2014 r o informowaniu o cenach towarów i usług (Dz. U. poz. 915).
2. Cena oferowana musi obejmować w kalkulacji wszystkie koszty i składniki, niezbędne do wykonania przedmiotu zamówienia min: koszt ubezpieczenia przedmiotu zamówienia, koszty załadunku i wyładunku, koszty transportu, itp. a w przypadku Wykonawcy spoza wspólnego obszaru celnego Unii Europejskiej również opłaty celne.
3. Wykonawca określa cenę realizacji zamówienia poprzez wskazanie w Formularzu ofertowym sporządzonym wg wzoru stanowiącego Załączniki nr 2 do SIWZ łącznej ceny ofertowej brutto za realizację przedmiotu zamówienia.
4. Zamawiający przewiduje możliwości zmian ceny ofertowej brutto w sytuacjach wymienionych w umowie.
5. Jeżeli w postępowaniu zostanie złożona oferta, której wybór prowadziłby do powstania obowiązku podatkowego Zamawiającego zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny, podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.
6. Cena oferty to cena brutto.
7. Cena jednostkowa towaru to cena ustalona za jednostkę określonego towaru, którego ilość lub liczba jest wyrażona w jednostkach miar, w rozumieniu przepisów o miarach
8. Ceny muszą być: podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
9. Cena oferty winna być wyrażona w złotych polskich (PLN).
10. Rozliczenia pomiędzy zamawiającym i Wykonawcą prowadzone będą w złotych polskich.
11. Zamawiający informuje, iż w treści oferty Wykonawcy poprawi w szczególności:
    1) omyłki polegające na błędnym wpisaniu ilości jednostek lub nazwy jednostki miary w treści złożonego przez Wykonawcę wraz z ofertą formularza cenowego, dostosowując ich treść do odpowiednich dokumentów wzorcowych zamieszczonych w specyfikacji istotnych warunków zamówienia;
    2) oczywiste omyłki rachunkowe polegające na błędnych obliczeniach matematycznych (mnożenie, dodawanie), a w konsekwencji wprowadzonych w ten sposób zmian poprawi końcową wartość oferty. Przy poprawianiu omyłek Zamawiający zawsze za prawidłową uzna cenę jednostkową netto.
    3) omyłki polegające na zdublowaniu tych samych pozycji w formularzu cenowym w następujący sposób:
    — zamawiający wykreśli z formularza cenowego zdublowane pozycje pozostawiając tylko jedną z nich;
    — po wykreśleniu zdublowanych pozycji Zamawiający zsumuje wartości podane w pozostawionych pozycjach formularza cenowego i tak obliczoną cenę przyjmie jako cenę ofertową;
    — w sytuacji kiedy zdublowane pozycje będą zawierać inne ceny Zamawiający wykreśli pozycję o wyższej cenie.

Wszelkie zamiany polegające na pominięciu jakiejkolwiek z istniejących w formularzu ofertowym pozycji (dotyczy to również podania wartości „0") nie będą uznane za możliwe do poprawienia w trybie art. 87 ust. 2 ustawy Pzp i skutkować będą odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy Pzp.

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

1. Za ofertę najkorzystniejszą zostanie uznana oferta zawierająca najkorzystniejszy bilans punktów w kryteriach:

   „Łączna cena ofertowa brutto" – C;

   „Termin realizacji dostawy" – T.

2. Powyższym kryteriom Zamawiający przypisał następujące znaczenie:

Kryterium	Waga [%]	Liczba punktów	Sposób oceny wg wzoru
Łączna cena ofertowa brutto	60%	60	$C = \frac{\text{Cena najtańszej oferty}}{\text{Cena badanej oferty}} \times 60\text{pkt}$
Okres gwarancji i wsparcia Systemu bezpieczeństwa	40%	40	$T = \frac{\text{Okres gwarancji i wsparcia Systemu bezpieczeństwa w badanej ofercie}}{\text{Najdłuższy zaoferowany okres gwarancji i wsparcia Systemu bezpieczeństwa}} \times 40\text{ pkt}$
RAZEM	100%	100	———

3. Całkowita liczba punktów, jaką otrzyma dana oferta, zostanie obliczona wg poniższego wzoru:

   L = C + G

   gdzie:

   L – całkowita liczba punktów,

   C – punkty uzyskane w kryterium „Łączna cena ofertowa brutto",

   G–punkty uzyskane w kryterium „Okres gwarancji i wsparcia Systemu bezpieczeństwa".

4. Ocena punktowa w kryterium „Łączna cena ofertowa brutto" dokonana zostanie na podstawie łącznej ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie i przeliczona według wzoru opisanego w tabeli powyżej.

5. Ocena punktowa w kryterium „Okres gwarancji i wsparcia Systemu bezpieczeństwa w badanej ofercie"

dokonana zostanie na podstawie **liczby m-cy** wskazanych przez Wykonawcę w ofercie, w których nastąpi dostawa Przedmiotu zamówieni i przeliczona według wzoru opisanego w tabeli powyżej.

6. Punktacja przyznawana ofertom w poszczególnych kryteriach będzie liczona z dokładnością do dwóch miejsc po przecinku. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.
7. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w Pzp, oraz w SIWZ i zostanie oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru.
8. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i pozostałych kryteriów oceny ofert, Zamawiający spośród tych ofert dokona wyboru oferty z niższą ceną.
9. Zamawiający nie przewiduje przeprowadzenia dogrywki w formie aukcji elektronicznej.

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

1. Przed podpisaniem umowy Wykonawca dostarczy Zamawiającemu dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
3. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający może żądać przed zawarciem umowy przedstawienia umowy regulującej współpracę tych Wykonawców. Umowa taka winna określać strony umowy, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdemu z nich, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania konsorcjum (obejmującego okres realizacji przedmiotu zamówienia, gwarancji i rękojmi), wykluczenie możliwości wypowiedzenia umowy konsorcjum przez któregokolwiek z jego członków do czasu wykonania zamówienia.
4. Zawarcie umowy nastąpi wg wzoru Zamawiającego.
5. Postanowienia ustalone we wzorze umowy nie podlegają negocjacjom.
6. W przypadku, gdy Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy, Zamawiający będzie mógł wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownego badania i oceny chyba, że zachodzą przesłanki, o których mowa w art. 93 ust. 1 Pzp.

Rozdział XVI. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

Rozdział XVII. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy.

Wzór umowy stanowi **Załącznik nr 4** do SIWZ.

Rozdział XVIII. Pouczenie o środkach ochrony.

1. Każdemu 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 PZP przysługują środki ochrony prawnej przewidziane w dziale VI ustawy PZP jak dla postępowań poniżej kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 Pzp.
2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 Pzp.

Rozdział XIX. Wykaz załączników do SIWZ

Załącznik nr 1 – Opis przedmiotu zamówienia;
Załącznik nr 2 – Formularz ofertowy;
Załącznik nr 3 – Oświadczenie;
Załącznik nr 4 – Projekt umowy;
Załącznik nr 5 – Wykaz dostaw.

AMW REWITA

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia

I. Opis przedmiotu zamówienia:

1. Przedmiotem zamówienia jest **dostawa, instalacja, konfiguracja oraz uruchomienie Systemu Bezpieczeństwa wraz ze szkoleniem pracownika wewnętrznego działu informatycznego, w skład którego wchodzi urządzenie typu UTM/NGFW, moduł ochrony systemu pocztowego oraz oprogramowanie pozwalające na centralne zarządzenie infrastrukturą informatyczną AMW Rewita Sp. z o.o.**
2. Oferent winien przedłożyć na etapie realizacji oświadczenie producenta oferowanego rozwiązania lub autoryzowanego dystrybutora oferowanego rozwiązania na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. Zamawiający wymaga, aby oferowane produkty były wolne od wad technicznych, prawnych i formalnych (m.in. aby pochodziły z autoryzowanych kanałów sprzedaży oraz nie były wcześniej zarejestrowane na żadnego innego klienta w bazie klientów danego producenta).
4. Oferta powinna uwzględniać wszystkie koszty związane z dostawą, montażem i uruchomieniem systemu bezpieczeństwa będącego przedmiotem zamówienia wraz z przeszkoleniem pracownika działu informatycznego Zamawiającego.
5. Zamawiający wymaga od Wykonawcy, aby przeprowadził szkolenie w Warszawie dla administratorów w zakresie administracji urządzeniem typu UTM/NGFW (wymagany co najmniej 1 dzień roboczy).
6. Zamawiający wymaga od wykonawcy, aby przeprowadził szkolenie w Warszawie dla administratorów w zakresie administracji modułem ochrony systemu pocztowego (wymagany co najmniej 1 dzień roboczy).
7. Zamawiający wymaga od wykonawcy, aby przeprowadził szkolenie w Warszawie dla administratorów w zakresie administracji systemem do centralnego zarządzania infrastrukturą (wymagany co najmniej 1 dzień roboczy).
8. Minimalny wymagany okres wsparcia – 36 miesięcy dla urządzenia typu UTM/NGFW oraz modułu ochrony systemu pocztowego. 36 miesięcy dla systemu do centralnego zarządzania infrastrukturą.

II. Minimalne warunki Systemu Bezpieczeństwa

Wymagania ogólne urządzenia typu UTM/NGFW

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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.

Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie

- System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45.
- System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe

1. W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 2 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1.400 Mbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 175 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 - zapora ogniowa 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, IMAP.
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.

2. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
3. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

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

Kontrola Antywirusowa

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

Ochrona przed atakami

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

Kontrola aplikacji

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

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 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 avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

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

Logowanie

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

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

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

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres co najmniej 36 miesięcy.

Gwarancja oraz wsparcie

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

Opisy do wymagań ogólnych

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

Moduł analityczny

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Interfejsy, Dysk:

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   - Listę najczęściej wykrywanych ataków.
   - Listę najbardziej aktywnych użytkowników.
   - Listę najczęściej wykorzystywanych aplikacji.
   - Listę najczęściej odwiedzanych stron www.
   - Listę krajów , do których nawiązywane są połączenia.
   - Listę najczęściej wykorzystywanych polityk Firewall.
   - Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.

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

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

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

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

III. Minimalne wymagania modułu ochrony systemu pocztowego

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu 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.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi być wyposażony w interfejsy:
   - 4 porty Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 500 GB.
3. System musi posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 50 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 2 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 2,5 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
7. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
8. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.

9. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
10. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
11. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
12. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
13. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
14. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
15. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.

14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.

2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 6 lokalnych kont administracyjnych.

Certyfikaty
VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę Antyspam, URL Filtering, kontrola antywirusowa na okres nie krótszy niż 36 miesięcy.

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

IV. Minimalne wymagania Oprogramowania do centralnego zarządzania infrastrukturą IT

Wymagania ogólne
1. Dostarczone licencje na oprogramowanie muszą być bezterminowe.
2. Dostarczone licencje na oprogramowanie muszą być dostarczone z rocznym supportem producenta, liczonym od daty zakończenia wdrożenia.
3. Obsługa serwisowa w zakresie błędów realizowana ma być z czasem reakcji 3 dni robocze oraz czasem naprawy 14 dni roboczych. W ramach supportu wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
4. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 150 stanowisk komputerowych oraz nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto muszą posiadać co najmniej 3 licencje dostępowe do konsoli zarządzającej
5. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
6. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
7. Oprogramowanie serwera aplikacji musi umożliwiać dystrybucję zadań oraz plików wg zaprojektowanej trasy przepływu danych z dedykowanego dla każdej lokalizacji repozytorium plików.
8. Oprogramowanie musi umożliwiać zaprojektowanie drzewiastej struktury przepływu danych (trasy) pomiędzy agentami a centralnym serwerem systemu.
9. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta poprzez lokalny odczyt WMI oraz bezpośredni dostęp do komponentów np. bezpośredni odczyt parametrów z BIOS'u komputera.

10. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do szyfrowanego pliku.
11. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
12. Oprogramowanie musi posiadać sprzętową obsługę jednoczesnych sesji operatorów konsoli (licencja pływająca) umożliwiającą jednoczesną pracę n-operatorów na wybranych instancjach zainstalowanych konsol zarządzających.
13. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
14. Oprogramowanie musi współpracować z serwerem MsSQL Server 2005/2008/2008R2/2012/2014.
15. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
16. Oprogramowanie musi posiadać przypisywanie wybranych jednostek organizacyjnych, Jednostek Lokalizacyjnych oraz typów zasobów do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko w/w przypisane obiekty.
17. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych widoków drzewiastych z danych dostępnych w systemie. Jeśli obiekt systemu jest w relacji z innym obiektem, to musi być możliwość zaprezentowania go w strukturze drzewa.
18. Oprogramowanie musi umożliwiać tworzenie kolumn w strukturze drzewiastej, w której jest możliwość umieszczenia dowolnej danej związanej z obiektem.
19. Oprogramowanie musi umożliwiać tworzenie wyrażeń w zakresie co najmniej funkcji zliczania obiektów podrzędnych wybranego typu w strukturze drzewiastej oraz sumowania ich wybranej właściwości liczbowej.
20. Oprogramowanie musi umożliwiać zapisywanie w bazie danych zbudowanych struktur widoków drzewiastych i udostępniania ich innym użytkownikom systemu.
21. Oprogramowanie musi umożliwiać eksport do Excela widoku drzewiastego od dowolnego obiektu w głąb, umożliwiając wybór konkretnych typów obiektów do eksportu.
22. Oprogramowanie musi być podpisane cyfrowo przez producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy każdego składnika Producenta systemu włączając w to pliki wykonywalne (*.exe), pliki bibliotek współdzielonych (*.dll), pliki sterowników (*.sys) oraz pliki paczek oprogramowania (*.msi).
23. Oprogramowanie musi realizować bezpośrednie zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej bez użycia wywoływanych widocznych interfejsów WWW.
24. Oprogramowanie agenta musi realizować wszystkie wymagane funkcjonalności za pomocą aplikacji lub usług wyprodukowanych i podpisanych cyfrowo przez Producenta bez użycia aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
25. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.

26. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min. : Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
27. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
28. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, grupy agentów, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
29. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/LDAP), kont użytkowników oraz komputerów wraz z zachowaniem ich oryginalnego położenia z możliwością tworzenia listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
30. Oprogramowanie musi posiadać kreator powiązań dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
31. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
32. Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
33. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
34. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
35. Oprogramowanie musi umożliwiać automatyczny odczyt informacji nt. uprawnień (ACL) do wybranych folderów z określonych grup stanowisk komputerowych (raport wg struktury organizacyjnej lub lokalizacyjnej).
36. Oprogramowanie musi umożliwiać automatyczny odczyt informacji nt. aktywnych lokalnych kont administracyjnych z określonych grup stanowisk komputerowych (raport wg struktury organizacyjnej lub lokalizacyjnej).
37. Oprogramowanie musi umożliwiać globalne uruchamianie skryptów PowerShell na wybranych grupach stanowisk komputerowych (wg struktury organizacyjnej lub lokalizacyjnej).

Minimalne wymagany zakresu funkcjonalności systemu:

1. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
2. Oprogramowanie musi umożliwiać analizę sprzętową:
   - płyty głównej w zakresie model, producent, nr. seryjny,
   - CPU w zakresie nazwy, modelu, producenta, częstotliwości,
   - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
   - RAM w zakresie wielkości pamięci,
   - karty sieciowej w zakresie model, adres IP, adres MAC,
   - karty graficznej w zakresie model.
3. Oprogramowanie musi posiadać wbudowany alerter, którego zadaniem jest cykliczne informowanie (poprzez e-mail) administratorów systemu o zmianach w zakresie konfiguracji sprzętowej, zmianach w oprogramowaniu (instalacja, dezinstalacja), kończących się okresach gwarancji zarządzanych zasobów (komputery, urządzenia dodatkowe), wygasaniu licencji na

oprogramowanie, informacje o planowanych przeglądach serwisowych, obciążenie pamięci RAM oraz zajętość dysków twardych.

4. Oprogramowanie musi posiadać filtry aktywności pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3 bez konieczności fizycznej obecności użytkownika przy stacji.
5. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
6. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
7. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie co najmniej nazwy BIOS, daty, producenta.
8. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
9. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
10. Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
11. Oprogramowanie musi umożliwiać zdefiniowanie dowolnego zasobu inwentaryzacyjnego (np. telefon, drukarka, nawigacja) wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
12. Oprogramowanie musi umożliwiać klonowanie wybranych typów zasobów
13. Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
14. Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
15. Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie : operator, data, czas, poprzednia oraz nowa wartość.
16. Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania stanowiska z pracownikiem, licencją, innym zasobem) wraz z zapisem historii relacji zasobów.
17. Oprogramowanie musi umożliwiać zdefiniowanie dodatkowych atrybutów dla wybranych relacji pomiędzy zasobami w zakresie zgodnym z atrybutami typów zasobów.
18. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
19. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych
20. w procesie automatycznego audytu licencji (rozliczenie ilościowe).
21. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
22. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
23. Oprogramowanie musi umożliwiać wykrywanie zmian w konfiguracji sprzętowej komputerów.

24. Oprogramowanie musi umożliwiać zapis dodatkowych informacji inwentaryzacyjnych dotyczących całego stanowiska komputerowego w zakresie numeru seryjnego komputera, numeru seryjnego monitora, numeru seryjnego drukarki, numeru seryjnego dowolnych urządzeń peryferyjnych,
25. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
26. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
27. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
28. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie : model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
29. Oprogramowanie musi umożliwiać import danych z zewnętrznego pliku CSV zawierającego informacje inwentaryzacyjne z nowo zakupionych urządzeń w zakresie : numer faktury, numer seryjny, model, nazwa, data zakupu.
30. Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
31. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
32. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
33. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
34. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
35. Oprogramowanie musi umożliwiać tworzenie zestawień duplikatów kluczy licencyjnych dotyczących zainstalowanego oprogramowania na komputerze.
36. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
37. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.
38. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
39. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
40. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem (wymagana w organizacji) wraz z możliwością raportowania wg w/w klasyfikacji.
41. Oprogramowanie musi umożliwiać okresowe skanowanie aktualnie uruchomionych procesów systemowych wraz z historią występowania procesu podczas wcześniejszych skanów.
42. Oprogramowanie musi umożliwiać analizę (aktualna oraz historyczna) średniego obciążenia CPU oraz transferu IO przez dowolnie wybrany proces w zadanych czasookresie.
43. Oprogramowanie musi umożliwiać zapisywanie informacji o procesach w bazie danych i powinny zawierać następujące informacje: nazwa procesu, lokalizacja, zajmowana pamięć, nazwa stanowiska gdzie po raz pierwszy wystąpił proces, data i czas wykrycia.

44. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
45. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury katalogowej, struktury sieciowej (pule IP) oraz własnego podziału.
46. Oprogramowanie musi umożliwiać dynamiczne zawężania wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
47. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
48. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
49. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
50. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
51. Oprogramowanie musi umożliwiać całkowitą interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska administratora stanowiska użytkownika, bez konieczności uprzedniego wylogowania użytkownika.
52. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego.
53. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
54. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
55. Oprogramowanie musi umożliwiać zdalną dwukierunkową linie poleceń.
56. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
57. Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
58. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
59. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
60. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
61. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych „local site servers") z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
62. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.

63. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
64. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
65. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
66. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
67. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
68. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.
69. Oprogramowanie musi umożliwiać generowanie wybranych raportów do pliku: PDF, CSV i Excel.
70. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).
71. Oprogramowanie musi umożliwiać globalny przegląd stanu zajętości dysków, obciążenia pamięci RAM oraz CPU w formie graficznych wykresów obejmujących wszystkie zarejestrowane w systemie stanowiska.
72. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem z zapisem historii konwersacji.
73. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
74. Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności :
    - Zarządzanie problemem
    - Zarządzanie incydentem
    - Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy)
    - Zarządzanie umowami serwisowymi
    - Definicje poziomów SLA (reakcja, naprawa, reklamacja)
75. Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, programowania i innych typów awarii zdefiniowanych przez administratora.
76. Portal WWW musi zostać dostarczony w technologii PHP w formie otwartych źródeł z możliwością samodzielnej edycji kodu.
77. Obsługa listy zgłoszeń serwisowych (incydentów i problemów) musi być realizowana z poziomu głównej konsoli systemu z zachowaniem sprzętowych procedur autoryzacji i nadanego poziomu uprawnień.
78. Oprogramowanie musi umożliwiać wykorzystanie bezpiecznego protokołu HTTPS.
79. Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
80. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.

81. Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmy SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
82. Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
83. Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
84. Oprogramowanie musi umożliwiać dodawanie przez administratora nowego wpisu historii, jak i umożliwia zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowego wpisu do zgłoszonego problemu wraz ze zmianą statusu.
85. Oprogramowanie musi umożliwiać administratorowi ustalanie statusów z zaznaczeniem, który ze statusów może używać użytkownik zgłaszający problem.
86. Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach statusu danego zgłoszenia.
87. Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
88. Zapisane przez administratora rozwiązania problemów i incydentów tworzą bazę wiedzy (powiązaną z kategoriami) Baza ta wyświetlana jest użytkownikom podczas przeglądania kategorii problemów. Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
89. Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
90. Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefonicznie informuje, że zepsuł mu się komputer).
91. Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
92. Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
93. Oprogramowanie musi umożliwiać informowanie pracowników o przestojach serwerach, awaria za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
94. Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). Możliwość powiązania każdej umowy z zakupionymi licencjami oprogramowania lub z zakupionym sprzętem.
95. Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
96. Oprogramowanie musi umożliwiać wiązanie wybranych incydentów w obsługę problemu wraz z automatycznym zamykaniem zgłoszeń powiązanych, zmianę statusu oraz obliczanie terminu realizacji.

97. Oprogramowanie musi zapewnić obsługę WorkFlow (obieg dokumentu w wersji elektronicznej) zintegrowany z system zgłoszeń serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych) przesyłu elektronicznych formularzy WWW wraz z możliwością samodzielnej edycji wyglądu formularza.
98. Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń, panel dla managera HelpDesk – analiza graficzna oraz tabelaryczna pracy operatorów HelpDesk).
99. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
100. Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW operatora HelpDesk informacji nt. aktywności zarejestrowanych stanowisk (on-line/off-line) oraz alertów dotyczących obciążenia CPU, RAM, HDD.
101. Na poziomie każdego węzła logicznego musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.
102. Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (n – godzin, n-dni)
103. Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń drogą mailową.
104. Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
105. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
106. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
107. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
108. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
109. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
110. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
111. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
112. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
113. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
114. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi
115. odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.

116. Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, rozmiar drukowanych stron.
117. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).
118. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
119. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
120. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
121. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
122. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
123. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
124. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.
125. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.
126. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB.
127. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
128. Oprogramowanie musi umożliwiać autoryzację wybranych urządzeń USB.
129. Oprogramowanie musi posiadać filtry aktywności pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3 bez konieczności fizycznej obecności użytkownika przy stacji.
130. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
131. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu : Grupa\Stanowisko\Zalogowany Użytkownik.
132. Oprogramowanie musi umożliwiać filtrację okresową oraz wg. grup stanowisk.
133. Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
134. Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
135. Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
136. Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
137. Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.

138. Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
139. Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
140. Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
141. Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
142. Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
143. Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
144. Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
145. Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.
146. Oprogramowanie musi umożliwiać indywidulaną konfigurację poziomów uprawnień zarejestrowanych użytkowników (pojedynczo lub zbiorowo) komunikatora z poziomu głównej konsoli zarządzającej (główna baza osobowa systemu ITSM)
147. Oprogramowanie musi umożliwiać delegowanie uprawnień do zarządzania konfiguracją oraz uprawnieniami komunikatora do wybranych operatorów głównej konsoli zarządzającej system ITSM.

AMW REWITA

Załącznik nr 2 do SIWZ

FORMULARZ OFERTOWY

OFERTA

złożona przez:

_____

ul. _____

00-000 _____

w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych na: **Dostawę i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o.,** (postępowanie nr: **RWT/PZP/9/2018)**

A. DANE WYKONAWCY:

Osoba upoważniona do reprezentacji Wykonawcy/ów i podpisująca ofertę:.....

Wykonawca/Wykonawcy.....

.....

Adres:.....

.....

Osoba odpowiedzialna za kontakty z Zamawiającym:.....

Dane teleadresowe na które należy przekazywać korespondencję związaną z niniejszym postępowaniem:

faks.....

e-mail.....

Adres do korespondencji (jeżeli inny niż adres siedziby): .....

Oświadczam, że zgodnie z kwalifikacją przedsiębiorstw prowadzę przedsiębiorstwo (proszę zaznaczyć właściwe):

mikro małe średnie duże

B. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

Dostawa i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o.,

C. ŁĄCZNA CENA OFERTOWA:

Niniejszym oferuję realizację przedmiotu zamówienia za ŁĄCZNĄ CENĘ OFERTOWĄ, która stanowi całkowite wynagrodzenie Wykonawcy, uwzględniające wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z SIWZ. Na łączną cenę brutto składają się ceny jednostkowe zaoferowane przeze mnie w Formularzu cenowo-ofertowym, który załączam do oferty.

ŁĄCZNA CENA OFERTOWA NETTO PLN:	
ŁĄCZNA CENA OFERTOWA BRUTTO PLN:	

AMW REWITA

D.

OKRES GWARANCJI I WSPARCIA SYSTEMU BEZPIECZEŃSTWA	..... miesięcy (należy podać ilość miesięcy)

E. **OŚWIADCZENIA:**

1) zamówienie zostanie zrealizowane w terminach określonych w SIWZ oraz ze wzorze umowy z uwzględnieniem szczegółowych warunków zamówienia.
2) w cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia;
3) zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia oraz wzorem umowy i nie wnosimy do nich zastrzeżeń oraz przyjmujemy warunki w nich zawarte;
4) uważamy się za związanych niniejszą ofertą przez okres **30 dni** licząc od dnia otwarcia ofert (włącznie z tym dniem);
5) akceptujemy warunki zapłaty wskazane we wzorze Umowy,
6) wadium* w wysokości .....PLN (słownie:......, zostało wniesione w dniu ....., w formie .....;
7) prosimy o zwrot wadium (wniesionego w pieniądzu), na zasadach określonych w art. 46 ustawy PZP, na następujący rachunek: .....;

*jeśli dotyczy

F. **ZOBOWIĄZANIA W PRZYPADKU PRZYZNANIA ZAMÓWIENIA:**

1) zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego;
2) osobą upoważnioną do kontaktów z Zamawiającym w sprawach dotyczących realizacji umowy jest .....
   e-mail:..... Tel./fax:.....

G. **SPIS TREŚCI:**

Integralną część oferty stanowią następujące dokumenty:

1) .....
2) .....

Oferta została złożona na ..... kolejno ponumerowanych stronach.

.....	.....
pieczęć Wykonawcy	Data i podpis upoważnionego przedstawiciela Wykonawcy

AMW REWITA

Załącznik nr 3 do SIWZ

OŚWIADCZENIE O BRAKU PODSTAW DO WYKLUCZENIA / I SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Przystępując do postępowania na **Dostawę i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o.**, (postępowanie nr: **RWT/PZP/9/2018)**

działając w imieniu Wykonawcy:

.....

(podać nazwę i adres Wykonawcy)

Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania i spełniam warunki udziału w postępowaniu.

W przedmiotowym postępowaniu Zamawiający zgodnie z art. 24 ust. 1 pkt. 12-23 ustawy PZP wykluczy:

1. Wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;
2. Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
   a) o którym mowa w art. 165a, art. 181–188, art. 189a, art. 218–221, art. 228–230a, art. 250a, art. 258 lub art. 270–309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2016 r. poz. 176),
   b) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny,
   c) skarbowe,
   d) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769);
3. Wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2;
4. Wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
5. Wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;

6. Wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;
7. Wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
8. Wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;
9. Wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
10. Wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2015 r. poz. 1212, 1844 i 1855 oraz z 2016 r. poz. 437);
11. Wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;
12. Wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

Ponadto Zamawiający przewiduje możliwość wykluczenia wykonawcy w sytuacji:

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 2015 r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615) 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 2015 r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016 r. poz. 615);
2) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
3) jeżeli Wykonawca lub osoby, o których mowa w ust. 1 pkt 14, uprawnione do reprezentowania wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 z:
   a) zamawiającym,
   b) osobami uprawnionymi do reprezentowania zamawiającego,

c) członkami komisji przetargowej,

d) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a

– chyba że jest możliwe zapewnienie bezstronności po stronie zamawiającego w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;

4) który z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;

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

Wykonawca ubiegający się o przedmiotowe zamówienie musi spełniać również warunki udziału w postępowaniu dotyczące: **posiadania zdolności technicznej lub zawodowej** określone przez Zamawiającego w Rozdziale V pkt. 1 ppkt 2) lit. c) SIWZ.

Informacja w związku z poleganiem na zasobach innych podmiotów

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w rozdziale V SIWZ polegam na zasobach następującego/ych podmiotu/ów:

_____

_____

_____

_____

_____

_____

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)

Oświadczenie dotyczące podmiotu, na którego zasoby powołuje się Wykonawca

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: ..... *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)* nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

Oświadczenie dotyczące podwykonawcy niebędącego podmiotem, na którego zasoby powołuje się Wykonawca

AMW REWITA

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, będącego/ych podwykonawcą/ami: ..... (podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG), nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.	
..... Pieczęć Wykonawcy	..... ata i podpis upoważnionego przedstawiciela Wykonawcy

A2

AMW REWITA

Załącznik nr 4 do SIWZ

Umowa nr .../2018
na dostawę i wdrożenie systemu bezpieczeństwa

zwana dalej **„Umową"**, zawarta w Warszawie w dniu .... 2018 roku, pomiędzy:

AMW REWITA Sp. z o.o. z siedzibą w Warszawie (03-310), przy ul. Św. Jacka Odrowąża 15, zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, Wydział XIII Gospodarczy KRS, pod numerem 0000394569, NIP 701-030-24-56, REGON 142990254, kapitał zakładowy 534 072 000,00 zł, reprezentowaną zgodnie z zasadami reprezentacji ujawnionymi w KRS, przez:

1. Damiana Pietrzyka – Prezesa Zarządu;
2. Elżbietę Cendrzak – Wiceprezes Zarządu;

zwaną dalej **„Zamawiającym"**,

a

w zależności od formy prawnej Wykonawcy uzupełnić jedno z poniższych)

..... z siedzibą w ..... (... - ....), przy ul. ....., zarejestrowaną w rejestrze przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd ....., Wydział ... Gospodarczy KRS, pod numerem ....., NIP ....., REGON ....., kapitał zakładowy w całości wniesiony i opłacony w wysokości ... zł, reprezentowaną zgodnie z zasadami reprezentacji ujawnionymi w KRS lub na podstawie pełnomocnictwa nr .... z dnia ..... roku, stanowiącego wraz z wydrukiem z KRS **Załącznik nr 1** do Umowy, przez:

1. ..... -.....;
2. ..... - .....;

..... prowadzącą/ym działalność gospodarczą pod firmą ....., z głównym miejscem wykonywania działalności oraz adresem do doręczeń w ..... (...-...), przy ul. ....., wpisaną/ym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP ....., REGON ....., reprezentowaną/m osobiście albo przez pełnomocnika przedsiębiorcy ujawnionego w CEIDG lub na podstawie pełnomocnictwa nr ..... z dnia ..... roku, stanowiącego wraz z wydrukiem z CEIDG
Załącznik nr 1 do Umowy;
zwaną dalej **„Wykonawcą"**,
zwane dalej pojedynczo **„Stroną"**, a łącznie **„Stronami"**.

Umowa została zawarta po przeprowadzeniu postępowania w trybie otwartym na podstawie regulaminu wewnętrznego Zamawiającego – **nr sprawy RWT/DO (ZI) 272 /REG/4/2018**, o następującej treści:

§ 1.
[Przedmiot Umowy]

1. Przedmiotem Umowy jest dostawa, instalacja, konfiguracja oraz uruchomienie systemu bezpieczeństwa, w skład którego wchodzi urządzenie typu UTM/NGFW, moduł ochrony systemu pocztowego oraz oprogramowanie pozwalające na centralne zarządzenie infrastrukturą informatyczną Zamawiającego (zwane dalej **„Systemem"**) wraz ze szkoleniem pracownika wewnętrznego działu informatycznego Zamawiającego.

2. Szczegółową ilość niezbędnych urządzeń do budowy Systemu oraz wymogi co do sposobu wykonania Umowy określono w Szczegółowym opisie przedmiotu zamówienia stanowiącym **Załącznik nr 2** do Umowy.
3. W ramach realizacji przedmiotu Umowy Wykonawca dostarczy niezbędne urządzenia oraz niezbędne licencje do wskazanego miejsca dostawy wraz z wdrożeniem i konfiguracją w środowisku IT Zamawiającego.
4. Wykonawca oświadcza, że posiada wszelkie wymagane koncesje, zezwolenia i uprawnienia do prowadzenia działalności w związku z przedmiotem Umowy oraz dysponuje stosownym doświadczeniem, możliwościami technicznymi oraz finansowymi do należytej realizacji Umowy.

§ 2.
[Pakowanie i znakowanie urządzeń oraz licencji, które wchodzą w skład Systemu]

1. Dostarczone urządzenia oraz licencje, które wchodzą w skład Systemu będą spełniały wymogi i zostaną oznaczone zgodnie z powszechnie obowiązującym prawem oraz będą posiadały wszelkie wymagane prawem atesty i świadectwa dopuszczające go do obrotu na terytorium Rzeczypospolitej Polskiej. W przypadku zmiany regulacji prawnych w trakcie trwania Umowy, System będzie spełniał wymagania aktualnie obowiązujących aktów.
2. Opakowanie urządzeń i licencji powinno być odpowiednie do rodzaju transportu i będzie chroniło je przed wszystkimi możliwymi warunkami, których można się spodziewać w czasie transportu. Wykonawca zobowiązany jest do należytego zabezpieczenia urządzeń na czas ich przewozu i ponosi całkowitą odpowiedzialność za ich dostarczenie, jakość i uszkodzenia powstałe w trakcie transportu. Wszelkie koszty związane z transportem i dostawą urządzeń zostały zawarte w wynagrodzeniu określonym w § 7 ust. 1 Umowy.

§ 3.
[Warunki dostawy]

1. Wykonawca dostarczy i wdroży zamawiany System wraz z niezbędnymi urządzeniami i licencjami do Biura Zarządu Zamawiającego w Warszawie (03-310), przy ul. Św. Jacka Odrowąża 15, w terminie nie dłuższym **niż 30** dni od dnia zawarcia Umowy.
2. Jakościowy odbiór zostanie dokonany przez przedstawiciela Zamawiającego i Wykonawcy w miejscu dostawy określonym w ust. 1 powyżej, w szczególności w oparciu o złożone zamówienie, fakturę, dokumenty dostawy i wszelkimi innymi wymaganymi przez obowiązujące prawo dokumentami m.in. świadectwami, certyfikatami i atestami.
3. Przekazanie działającego Systemu nastąpi na podstawie protokołu zdawczo-odbiorczego Wzór protokołu stanowi **Załącznik nr 3** do Umowy. Jedynie podpisanie przez Strony protokołu zdawczo-odbiorczego kompletnego przedmiotu Umowy bez uwag stanowi dowód wykonania przez Wykonawcę przedmiotu Umowy, a data jego podpisania oznacza datę wykonania Umowy.

§ 4.
[Gwarancja i rękojmia]

1. Wykonawca oświadcza, że dostarczone urządzenia oraz licencje niezbędne do prawidłowego działania Systemu są wolne od wad fizycznych i prawnych oraz może być użytkowany zgodnie z przeznaczeniem.
2. Wykonawca oświadcza, że System oparty na urządzeniach typu UTM/NGFW oraz ochrona poczty jest objęta …. miesięczną gwarancją oraz wsparciem producenta. Moduł do centralnego zarządzania infrastrukturą IT jest objęty …. miesięczną gwarancją oraz suportem producenta. Termin gwarancji rozpoczyna bieg w dniu następnym po dniu dokonania odbioru przedmiotu Umowy.

3. Jeżeli w ramach gwarancji Wykonawca dokonał usunięcia wad istotnych, termin gwarancji biegnie na nowo od chwili usunięcia wady. W innych wypadkach termin gwarancji ulega przedłużeniu o czas, w którym wada była usuwana.
4. Jeżeli z powodu wady prawnej Systemu Zamawiający będzie zmuszony wydać go osobie trzeciej, Wykonawca jest obowiązany do zwrotu otrzymanej kwoty bez względu na inne postanowienia Umowy.
5. Jeżeli Wykonawca nie przystąpi we właściwym terminie do usunięcia wady oraz naprawienia szkód wyrządzonych taką wadą, wówczas Zamawiający może, po zawiadomieniu o tym Wykonawcy, usunąć taką wadę i naprawić wyrządzone szkody we własnym zakresie i na koszt Wykonawcy. Zamawiającemu będzie przysługiwać takie uprawnienie również w sytuacji, jeśli Wykonawca rozpocznie usuwanie wady wraz
z wyrządzoną szkodą, lecz je bezzasadnie wstrzyma lub też ich nie ukończy we właściwym terminie. Koszty usunięcia wady wraz z wyrządzoną szkodą zostaną w takim przypadku zwrócone Zamawiającemu w całości przez Wykonawcę w terminie 7 dni od dnia otrzymania żądania Zamawiającego w tej kwestii.

§ 5.
[Osoby odpowiedzialne za realizację Umowy]

1. Strony wyznaczają niżej wymienione osoby, jako osoby uprawnione do kontaktowania się w związku z realizacją Umowy:
   a) w imieniu Zamawiającego – Rafał Lenarczyk tel.: 22 270 9597, r.lenarczyk@rewita.pl;
   b) w imieniu Wykonawcy – ……., ……..r , tel. ……., ……@……..
2. Każda ze Stron ma prawo do zmiany w każdym czasie osoby odpowiedzialnej za realizację Umowy po jej stronie. Zmiana taka nie wymaga zmiany Umowy, wymaga jednak uprzedniego poinformowania o tym drugiej Strony, pod rygorem nieważności ustaleń poczynionych między dotychczasowymi osobami. Osoby odpowiedzialne mają prawo do składania wszelkich oświadczeń związanych z realizacją Umowy, za wyjątkiem składania oświadczeń woli.

§ 6.
[Wynagrodzenie]

1. Wynagrodzenie Wykonawcy za wykonanie Przedmiotu Umowy ma charakter ryczałtowy i wynosi: netto …… PLN (słownie: ……., ……../100), tj. wartość brutto ……. PLN (słownie: ……., …/100).
2. Wynagrodzenie obejmuje wszelkie koszty związane z realizacją postanowień Umowy, w tym koszt urządzeń, licencji, wszelkie koszty związane z jego dostarczeniem do miejsca dostawy, wdrożeniem oraz szkoleniem, należne podatki, opakowania oraz wszelkie inne koszty niewymienione, a niezbędne do właściwej realizacji przedmiotu Umowy.
3. Wykonawca zobowiązuje się dostarczyć Zamawiającemu wraz z Systemem dokumenty dostawy oraz wszelkie inne wymagane przez obowiązujące prawo dokumenty m.in. świadectwa, certyfikaty i atesty.
4. Po podpisaniu przez Strony końcowego protokołu odbioru, Wykonawca wystawi fakturę i dostarczy ją Zamawiającemu niezwłocznie, w terminie nie dłuższym niż 5 dni od dnia wystawienia.
5. Zamawiający zobowiązuje się zapłacić przelewem cenę za dostarczony System w terminie 30 dni od dnia otrzymania prawidłowo wystawionej faktury. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.
6. W przypadku błędnego podania na fakturze numeru rachunku bankowego przez Wykonawcę, koszty związane z dokonaniem ponownego przelewu, którymi bank obciąży Zamawiającego, poniesie Wykonawca.

§ 7.
[Termin realizacji Umowy]

1. Umowa została zawarta na czas jej realizacji, tj. do dnia …….. 2018 roku.
2. Zamawiający zastrzega sobie prawo do jednostronnego przesunięcia terminu dostawy Systemu o okres 10 dni, w sytuacji zaistnienia przyczyn od Zamawiającego niezależnych, o czym Wykonawca zostanie poinformowany pisemnie. Skorzystanie przez Zamawiającego z prawa przesunięcia terminu dostawy nie wymaga zmiany Umowy.

§ 8.
[Odstąpienie od Umowy]

1. Zamawiający jest uprawniony do odstąpienia od Umowy w przypadku wystąpienia jednej z niżej wymienionych przesłanek:
   a) uchybienia przez Wykonawcę terminu dostawy;
   b) naruszenia norm jakościowych i ilościowych dostarczonych licencji, niezbędnych urządzeń wchodzących w skład Systemu;
   c) zaniechania realizacji dostawy;
   d) wydania nakazu zajęcia majątku Wykonawcy;
   e) zaistnienia okoliczności, ze względu których jest wątpliwe, czy Wykonawca ma możliwość realizować przedmiot Umowy, np. istnieją przesłanki by wszcząć postępowanie upadłościowe, restrukturyzacyjne lub likwidacyjne przedsiębiorstwa Wykonawcy.
2. W przypadku wystąpienia przesłanek określonych w ust. 1 lit a), b) i c) powyżej Zamawiający uprzednio wezwie Wykonawcę do zaprzestania naruszeń, zaś w przypadku określonym w ust. 1 lit d) i e) Zamawiający może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
3. Odstąpienie umowne opisane w ustępach poprzedzających nie ogranicza prawa Zamawiającego do odstąpienia od Umowy na zasadach przewidzianych w kodeksie cywilnym. W przypadku odstąpienia umownego lub na podstawie kodeksu cywilnego, Wykonawca ma prawo wyłącznie do wynagrodzenia należnego za wykonaną i potwierdzoną przez Zamawiającego część Umowy.

§ 9.
[Kary umowne]

1. Wykonawca zapłaci Zamawiającemu karę umowną w przypadku:
   1) odstąpienia od Umowy przez którąkolwiek ze Stron z winy Wykonawcy w wysokości 20% wynagrodzenia brutto, o którym mowa w § 6. ust. 1 Umowy, tj. ……. PLN (słownie: …. złotych, ../100);
   2) niedostarczenia licencji, niezbędnych urządzeń wchodzących w skład Systemu lub niewykonania szkolenia pracownika Zamawiającego przez Wykonawcę w terminie i miejscu ustalonym przez Strony - w wysokości 500 PLN za każdy rozpoczęty dzień;
   3) dostarczenia licencji, niezbędnych urządzeń wchodzących w skład Systemu lub niewykonania szkolenia pracownika Zamawiającego przez Wykonawcę po upływie terminu określonego w Umowie – w wysokości 500 PLN za każdy rozpoczęty dzień zwłoki;
   4) dostarczenia licencji, niezbędnych urządzeń wchodzących w skład Systemu lub niewykonania szkolenia pracownika Zamawiającego przez Wykonawcę z wadami - w wysokości 500 PLN za każdy przypadek, za każdą wadę;
   5) zwłoki w wykonaniu obowiązków wynikających z gwarancji lub rękojmi - w wysokości 500 PLN
   za każdy rozpoczęty dzień zwłoki, za każdy przypadek.
2. W przypadkach określonych w ust. 1 lit c), d) i e) kary umowne podlegają łączeniu.

3. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania na zasadach ogólnych przewidzianych w kodeksie cywilnym w przypadku, jeśli szkoda wynikła z niewykonania lub nienależytego wykonania Umowy przewyższa wartość zastrzeżonej kary umownej bądź wynika z innych tytułów niż zastrzeżone.
4. Wykonawca wyraża zgodę na potrącenie kar umownych należnych Zamawiającemu na mocy powyższych postanowień z należności za dostawę Systemu.

§ 10.
[Postanowienia końcowe]

1. Przeniesienie praw i obowiązków Wykonawcy wynikających z Umowy na osoby trzecie wymaga uprzedniej pisemnej zgody Zamawiającego.
2. Zarówno treść Umowy, jak wszelkie informacje uzyskane przy okazji lub w związku z wykonywaniem Umowy, a dotyczące Zamawiającego stanowią informacje poufne, za wyjątkiem informacji powszechnie znanych lub udostępnionych przez Zamawiającego. Wykonawca zobowiązuje się do ich nieudostępniania osobom trzecim, bezpośrednio i pośrednio, bez względu na formę, bez uprzedniej, wyraźnej zgody Zamawiającego – przez czas trwania Umowy oraz po jej ustaniu. W przypadku udostępnienia informacji, na żądanie organu państwowego, Wykonawca zobowiązuje się do niezwłocznego poinformowania Zamawiającego o tym fakcie, zakresie i formie udostępnienia.
3. Wszelkie oświadczenia woli winny być kierowane na piśmie listem poleconym na adresy wskazane w komparycji Umowy. Zmiana adresu nie wymaga zmiany Umowy, aczkolwiek w razie niepoinformowania drugiej Strony o zmianie adresu, doręczenie dokonane na adres dotychczasowy uznaje się za skuteczne.
4. Wszelkie zmiany, rozwiązanie lub odstąpienie od Umowy wymaga formy pisemnej pod rygorem nieważności.
5. Spory powstałe w związku z realizacją Umowy będą rozstrzygane przez sąd właściwy miejscowo dla siedziby Zamawiającego.
6. W sprawach nieuregulowanych Umową stosuje się odpowiednie przepisy kodeksu cywilnego.
7. Wszelkie załączniki do Umowy, stanowią jej integralną część.
8. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Lista załączników:

1. Załącznik nr 1 – aktualny wydruk z KRS Wykonawcy;
2. Załącznik nr 2 – Szczegółowy opis przedmiotu zamówienia;
3. Załącznik nr 3 – Wzór protokołu zdawczo-odbiorczego.

Zamawiający	**Wykonawca**
.....	.....
(pieczątka i podpis)	*(pieczątka i podpis)*
.....	.....
(pieczątka i podpis)	*(pieczątka i podpis)*

AMW REWITA

(W zależności od rodzaju umowy, podpisuje właściwa jednostka organizacyjna)

Departament Prawny	Departament Nieruchomości	Departament Organizacyjny	Departament Finansów	Departament Kadr	Departament Promocji

AMW REWITA

Załącznik nr 5 do SIWZ

.....
Pieczęć Wykonawcy

.....
Miejscowość, data

WZÓR WYKAZU DOSTAW*

Dotyczy: postępowania o udzielenie zamówienia publicznego **na Dostawę i wdrożenie Systemu Bezpieczeństwa dla AMW REWITA Sp. z o.o., (postępowanie nr: RWT/PZP/9/2018)**

W zakresie niezbędnym do wykazania spełniania warunku posiadania zdolności technicznej lub zawodowej, w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy — w tym okresie, wykonaliśmy następujące dostawy.

Lp.	**Przedmiot dostawy**	**Wartość brutto dostaw**	Data **wykonania** (zakończenia umowy)	**Podmiot, na rzecz którego dostawy zostały wykonane**
W zakresie dostaw urządzenia typu UTM/NGFW, o wartości co najmniej 45 000,00 zł każda				
1				
2				
W zakresie dostaw modułu ochrony systemu pocztowego, o wartości co najmniej 30 000,00 zł każda				
1				
2				
W zakresie dostaw oprogramowania do centralnego zarządzania infrastrukturą IT, obejmujących co najmniej 150 stacji każda				
1				
2				

.....
data i podpis upoważnionego przedstawiciela Wykonawcy

*do wykazu należy dołączyć dokumenty potwierdzające należyte wykonanie wymienionych w wykazie dostaw