

Warszawa, 20 lipca 2020 r.

ZATWIERDZAM

**ZASTĘPUJĄCY DYREKTORA GENERALNEGO
Urzędu Patentowego Rzeczypospolitej Polskiej
Marcin Brzozowski**

**SPECYFIKACJA ISTOTNYCH
WARUNKÓW ZAMÓWIENIA**

Nr sprawy BG-II.211.19.2020

Tryb postępowania:	PRZETARG NIEOGRANICZONY (art. 39 i nast. ustawy Prawo zamówień publicznych)
Przedmiot:	Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu.
Zamawiający:	URZĄD PATENTOWY RZECZYPOSPOLITEJ POLSKIEJ 00-950 Warszawa, al. Niepodległości 188/192

WPROWADZENIE

1. Postępowanie prowadzone jest na podstawie ustawy z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 ze zmian.), zwanej dalej „ustawą Pzp”.
2. Wykonawca powinien przesłać ofertę zgodnie z postanowieniami niniejszej Specyfikacji Istotnych Warunków Zamówienia (SIWZ).

I. NAZWA I ADRES ZAMAWIAJĄCEGO

Urząd Patentowy Rzeczypospolitej Polskiej
00-950 Warszawa, al. Niepodległości 188/192.
<https://uprp.gov.pl>

II. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie jest prowadzone w trybie przetargu nieograniczonego na podstawie art. 39 ustawy Pzp i nast. odnoszących się do zamówień, których wartość szacunkowa nie przekracza kwot określonych w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup usługi wsparcia producenckiego dla działającego w Urzędzie Patentowym Rzeczypospolitej Polskiej systemu antywirusowego Symantec Endpoint Protection oraz rozbudowa tego systemu do 900 licencji, zapewniających jednoczesną ochronę antywirusową serwerów i stacji roboczych ważną do dnia co najmniej 01.08.2023.
2. W ramach usługi wsparcia Wykonawca, w uzgodnionym z Zamawiającym terminie, przeprowadzi przegląd ukierunkowany na optymalizację konfiguracji dostarczanego systemu antywirusowego w zakresie określonym w OPZ.

Szczegółowy Opis przedmiotu zamówienia został zawarty w Załączniku nr 1 do SIWZ.

Nazwy i kody Wspólnego Słownika Zamówień:

Usługi w zakresie wsparcia technicznego – 72611000-6

Pakiety oprogramowania i systemy informatyczne – 48000000-8

IV. OPIS CZĘŚCI ZAMÓWIENIA, JEŻELI ZAMAWIAJĄCY DOPUSZCZA SKŁADANIE OFERT CZĘŚCIOWYCH/ LICZBA CZĘŚCI ZAMÓWIENIA, NA KTÓRĄ WYKONAWCA MOŻE ZŁOŻYĆ OFERTĘ LUB MAKSYMALNĄ LICZBĘ CZĘŚCI, NA KTÓRE ZAMÓWIENIE MOŻE ZOSTAĆ UDZIELONE TEMU SAMEMU WYKONAWCY, ORAZ KRYTERIA LUB ZASADY, KTÓRE BĘDĄ MIAŁY ZASTOSOWANIE DO USTALENIA, KTÓRE ZAMÓWIENIA ZOSTANĄ UDZIELONE JEDNEMU WYKONAWCY, W PRZYPADKU WYBORU JEGO OFERTY W WIĘKSZEJ NIŻ MAKSYMALNA LICZBIE CZĘŚCI

Zamawiający nie dopuszcza składania ofert częściowych.

V. INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 67 UST. 1 PKT 6 I 7 LUB ART. 134 UST. 6 PKT 3, JEŻELI ZAMAWIAJĄCY PRZEWIDUJE

UDZIELENIE TAKICH ZAMÓWIEŃ

Zamawiający nie przewiduje zamówień, o których mowa w art. 67 ust. 1 pkt 6 i 7 ustawy Pzp.

VI. OPIS SPOSOBU PRZEDSTAWIANIA OFERT WARIANTOWYCH ORAZ MINIMALNE WARUNKI, JAKIM MUSZĄ ODPOWIEDAĆ OFERTY WARIANTOWE WRAZ Z WYBRANYMI KRYTERIAMI OCENY, JEŻELI ZAMAWIAJĄCY DOPUSZCZA ICH SKŁADANIE

Zamawiający nie dopuszcza składania ofert wariantowych.

VII. PODWYKONAWSTWO

1. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych części zamówienia.
2. Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców.

VIII. TERMIN WYKONANIA ZAMÓWIENIA

Zamówienie będzie realizowane w terminie:

do 12 dni - dostarczenie numeru umowy serwisowej i rozbudowa systemu,

do dnia 1.08.2023 r. r. - usługa wsparcia

IX. WARUNKI UDZIAŁU W POSTĘPOWANIU

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy

- nie podlegają wykluczeniu
- spełniają warunki udziału w postępowaniu

X. PODSTAWY WYKLUCZENIA

1. Z postępowania o udzielenie zamówienia wyklucza się wykonawcę, w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 24 ust. 1 pkt 12-23 ustawy Pzp.
2. Wykluczenie wykonawcy następuje zgodnie z art. 24 ust. 7 -12 ustawy Pzp.

XI. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW WYKLUCZENIA

1. Do oferty wykonawca zobowiązany jest dołączyć aktualne na dzień składania ofert oświadczenie stanowiące wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. *Wzór oświadczenia stanowi Załącznik nr 3 i Załącznik nr 4 do SIWZ.*
2. Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp, przekazuje zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. *Wzór oświadczenia stanowi Załącznik nr 5 do SIWZ.*

3. Zamawiający, zgodnie z art. 24aa ustawy Pzp, w pierwszej kolejności dokona oceny ofert, a następnie zbada czy wykonawca, którego oferta została oceniona jako najkorzystniejsza nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

XII. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, żaden z nich nie może podlegać wykluczeniu z powodu niespełniania warunków, o których mowa w art. 24 ust. 1 ustawy Pzp.
3. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w pkt. XI ust. 1, składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.
4. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o którym mowa w pkt. XI ust. 2, składa każdy z Wykonawców.

XIII. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, JEŻELI ZAMAWIAJĄCY, W SYTUACJACH OKREŚLONYCH W ART. 10C-10E, PRZEWIDUJE INNY SPOSÓB POROZUMIEWANIA SIĘ NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawca przekazują pisemnie, faksem lub drogą elektroniczną, w tym, za pośrednictwem systemu Marketplanet, o którym mowa w punkcie B poniżej.

A. Korespondencja poza systemem Marketplanet

1. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub mailem, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
2. Domniemywa się, że pismo wysłane przez Zamawiającego na numer faksu podany przez Wykonawcę zostało mu doręczone w sposób umożliwiający zapoznanie się Wykonawcy z treścią pisma, chyba, że Wykonawca wezwany przez Zamawiającego do potwierdzenia otrzymania oświadczenia, wniosku, zawiadomienia lub informacji w sposób określony w punkcie 2 oświadczy, że ww. wiadomości nie otrzymał.
3. Korespondencję związaną z niniejszym postępowaniem należy kierować na adres:
Urząd Patentowy RP, al. Niepodległości 188/192, 00-950 Warszawa,
faks Zamawiającego 22 57 90 373,

e-mail: **wzp1920@uprp.gov.pl**

4. Do porozumiewania się z Wykonawcą w sprawach związanych z postępowaniem upoważnieni są:

- Włodzimierz Kućko– tel. 22 57 90 456 w sprawach merytorycznych;
- Beata Sokołowska-Odeh– tel. 22 57 90 349 w sprawach proceduralnych.

B. Korespondencja za pośrednictwem Systemu Marketplanet

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami, w szczególności składanie ofert oraz oświadczeń, odbywa się również (opcjonalnie dla wykonawców) przy użyciu środków komunikacji elektronicznej zapewnionych za pośrednictwem Platformy przez system Marketplanet („System” lub „Platforma”). System jest dostępny pod adresem: <https://uprp.ezamawiajacy.pl>
2. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Instrukcji dla Wykonawców korzystających z Systemu.
3. Niezbędne wymagania sprzętowo - aplikacyjne umożliwiające komunikację pomiędzy Zamawiającym a Wykonawcą, w przypadku korzystania z Systemu:
 - 1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s;
 - 2) komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min 2GB Ram, procesor Intel IV 2GHZ, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10.4, Linux, lub ich nowsze wersje;
 - 3) zainstalowana dowolna przeglądarka internetowa obsługująca TLS 1.2, najlepiej w najnowszej wersji w przypadku Internet Explorer minimalnie wersja 10.0;
 - 4) włączona obsługa JavaScript;
 - 5) dokumenty w formacie pdf. zaleca się podpisywać formatem PAdES;
 - 6) zainstalowany program Acrobat Reader lub inny obsługujący pliki w formacie .pdf.
4. Dopuszczalna wielkość plików przesyłanych za pośrednictwem Platformy wynosi do 75 MB.
5. W celu zapoznania się z dokumentacją postępowania dostępną w Systemie (na Platformie zakupowej) Wykonawca korzysta z zakładki „Lista ogłoszeń o postępowaniach” i wybiera zakładkę „Aktualne” i wyszukuje przedmiotowe postępowanie a następnie klikając w wiersz postępowania, przechodzi do obszaru postępowania. Wykonawca ma możliwość pobrania każdego dokumentu odrębnie po naciśnięciu na wybrany załącznik lub w formie skompresowanej paczki po zaznaczeniu wybranych dokumentów. Po upływie terminu składania ofert przechodzi do zakładki „Lista ogłoszeń o postępowaniach”, wybiera zakładkę „Archiwalne”, wyszukuje przedmiotowe postępowanie, a następnie klikając w wiersz postępowania, przechodzi do obszaru postępowania.
6. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem Systemu po zalogowaniu się przez Wykonawcę na konto użytkownika, w zakładce „Korespondencja”. Wykonawcy, w celu bezproblemowej komunikacji z Zamawiającym na Platformie powinni przed upływem terminu składania ofert przystąpić do postępowania na Platformie poprzez funkcjonalność „Przystąpienie do postępowania” oraz posiadać założone konto w aplikacji Marketplanet OnePlace. Po przystąpieniu do postępowania Platforma przekieruje wykonawcę na stronę logowania się. W celu zalogowania się należy podać dane użytkownika: e-mail oraz hasło. W przypadku, gdy Wykonawca nie posiada konta użytkownika, wypełnia formularz rejestracyjny dostępny po kliknięciu funkcjonalności „Założ konto za darmo”. Następnie Wykonawca postępuje zgodnie

ze wskazówkami Marketplanet OnePlace, które otrzyma na wskazany w formularzu rejestracyjnym adres e-mail. Założenie konta Wykonawcy w aplikacji Marketplanet OnePlace wymaga akceptacji „Regulaminu korzystania z Marketplanet OnePlace”.

7. Sposób sporządzania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia.
8. Składanie w Systemie wniosków o wyjaśnienie treści SIWZ w trybie art. 38 ust. 1 ustawy Pzp następuje z wykorzystaniem funkcjonalności „Zadaj pytanie” (i nie wymaga logowania się w Systemie). W celu zadania pytania Zamawiającemu, Wykonawca po wejściu na stronę dotyczącą postępowania klika lewym przyciskiem myszy opcję „Zadaj pytanie”, co powoduje otwarcie okna, w którym należy uzupełnić pola oznaczone czerwoną gwiazdką: adres e-mail i nazwa podmiotu pytającego, temat i treść pytania. Platforma umożliwia również załączenie pliku. Po wypełnieniu wskazanych pól wraz z wymaganym kodem weryfikującym z obrazka Wykonawca klika „Potwierdź”. Wykonawca uzyskuje potwierdzenie wysłania pytania poprzez komunikat systemowy przesłany na podany adres e-mail "Pytanie wysłane". W przypadku wykonawców zalogowanych w Systemie przesłanie pytania możliwe jest poprzez zakładkę „Pytania i odpowiedzi” dostępną po przejściu do postępowania.
9. Zapytania i odpowiedzi dotyczące treści SIWZ będą publikowane na stronie internetowej Zamawiającego oraz w Systemie.
10. Osobą wyznaczoną do kontaktu w sprawie postępowania jest Beata Sokołowska-Odeh, tel. + 48 22 57 90 349, e-mail: wzp120@uprp.gov.pl
11. Postępowanie jest prowadzone w języku polskim. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

XIV. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie żąda wadium.

XV. TERMIN ZWIĄZANIA OFERTĄ

Termin związania ofertą wynosi 30 dni licząc od dnia upływu terminu składania ofert.

XVI. OPIS SPOSOBU PRZYGOTOWANIA OFERT

1. Oferta powinna zawierać:
 - 1) Formularz ofertowy (wzór formularza stanowi Załącznik nr 2);
 - 2) Oświadczenia wymienione w pkt. XI ust. 1 SIWZ, (wzory formularzy stanowią Załączniki nr 3 i 4 do SIWZ);
 - 3) Pełnomocnictwo (jeżeli upoważnienie do reprezentacji podmiotu nie wynika z dokumentów rejestrowych);
2. Wykonawca, **w terminie 3 dni** od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp, przekazuje zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w

art. 24 ust. 1 pkt 23 ustawy Pzp. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. *Wzór oświadczenia stanowi Załącznik nr 5 do SIWZ.*

3. Ofertę należy sporządzić zgodnie z wymaganiami określonymi w Specyfikacji Istotnych Warunków Zamówienia.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Ofertę oraz oświadczenie, o którym mowa w ust. 2 należy złożyć **w jednej** z dwóch form (czyli **albo** w formie pisemnej **albo** w formie elektronicznej):

A. w formie pisemnej (papierowej):

1. Ofertę należy sporządzić w języku polskim, czytelnym pismem (wskazany jest maszynopis lub wydruk komputerowy).
2. Formularz ofertowy oraz oświadczenia powinny być podpisane przez osobę upoważnioną do reprezentowania firmy, zgodnie z formą reprezentacji wykonawcy określoną w rejestrze sądowym lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy. Wszystkie miejsca, w których wykonawca naniósł zmiany, winny być parafowane przez osobę podpisującą ofertę albo przez osobę umocowaną przez osoby uprawnione, przy czym umocowanie (pełnomocnictwo) musi być załączone do oferty. Pełnomocnictwo może być złożone w formie oryginału lub kopii poświadczonej za zgodność z oryginałem notarialnie.
3. Wykonawcy ubiegający się wspólnie o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Stosowne pełnomocnictwo powinno być dołączone do oferty w oryginale lub kopii poświadczonej za zgodność z oryginałem notarialnie.
4. Zaleca się aby każda kartka oferty była ponumerowana kolejnymi numerami i parafowana, a w formularzu ofertowym znajdowała się informacja z ilu kolejno ponumerowanych kartek składa się oferta wraz z załącznikami.
5. Zaleca się aby kartki oferty były trwale ze sobą połączone (np. zbindowane, zszyte), z zastrzeżeniem sytuacji opisanej w ust.6.
6. Informacje składane w trakcie postępowania, stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, co do których wykonawca zastrzega, że nie mogą być udostępniane innym uczestnikom postępowania, muszą być oznaczone klauzulą: Dokument stanowi tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r., Nr 153 poz. 1503 z późn. zm.) Informacje te winny być umieszczone w innej osobnej wewnętrznej kopercie, odrębnie od pozostałych informacji zawartych w ofercie. Kartki należy ponumerować w taki sposób, aby umożliwić ich dopasowanie do pozostałej części oferty (należy zachować ciągłość numeracji kartek oferty). W szczególności, zgodnie z art. 86 ust. 4 ustawy Pzp, nie można zastrzec informacji ogłoszonych w trakcie otwarcia ofert.
7. Wykonawca, który zastrzegł informacje zgodnie z punktem 6 powyżej, zobowiązany jest do wykazania w ofercie, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
8. Ofertę wraz ze wszystkimi załącznikami należy umieścić w zamkniętej kopercie. Kopertę należy zaadresować i opisać według poniższego wzoru:

Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu"

Nr sprawy BG-II.211.19.2020

Kopertę należy również opatrzyć dokładną nazwą i adresem Wykonawcy.

B. w formie elektronicznej:

1. Ofertę (z załącznikami) należy złożyć w języku polskim, sporządzoną pod rygorem nieważności, w postaci elektronicznej **opatrzoną kwalifikowanym podpisem elektronicznym**, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne – podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.
2. Ofertę elektroniczną należy złożyć (wyłącznie) za pośrednictwem Systemu (Platformy zakupowej) dostępnego pod adresem: <https://uprp.ezamawiajacy.pl>
3. W przypadku podpisywania oferty (odnosi się także do załączników) podpisem zewnętrznym Wykonawca spakuje pliki w jedno archiwum i spakowany plik umieści w Systemie wskazanym w ust. 2.
4. Ofertę należy sporządzić w w formacie danych txt, .rtf, .pdf, .odt, .ods, .doc, .docx, .xls, .xlsx, .xps, i podpisać kwalifikowanym podpisem elektronicznym. Sposób złożenia oferty, w tym zaszyfrowania oferty opisany został w Instrukcji dla Wykonawców korzystających z Platformy. Zamawiający zaleca stosowanie formatu pdf. Do kompresji dokumentów Zamawiający dopuszcza formaty .zip i .zip7.
5. Oferta musi być podpisana kwalifikowanym podpisem elektronicznym przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy. Po prawidłowym przekazaniu plików oferty wyświetlana jest informacja o pozytywnym przyjęciu oferty do Systemu.
6. Złożenie oferty w postępowaniu o udzielenie zamówienia publicznego wymaga zalogowania się wykonawcy na Platformie poprzez aplikację Marketplanet OnePlace <http://oneplace.marketplanet.pl>. Do złożenia oferty wystarczające jest założenie bezpłatnego konta BASIC. Instrukcja założenia konta zawarta jest na Platformie w zakładce „Regulacje i procedury procesu zakupowego”. Patrz także: pkt. XIII lit. B ust. 6 SIWZ.
7. Po zalogowaniu w Systemie i przejściu do postępowania wykonawca przechodzi do zakładki „Oferty”. Następnie wykonawca wypełnia poszczególne sekcje formularza elektronicznego oferty. Wykonawca ma możliwość dodania dokumentów, oświadczeń, pełnomocnictw jako załączników. Wszystkie załączniki wykonawca podpisuje kwalifikowanym podpisem elektronicznym poza Platformą. Załączenie dokumentów następuje poprzez polecenie „dodaj dokument” i wybranie docelowego pliku, który ma zostać wczytany. Wykonawca winien opisać każdy załącznik nazwą umożliwiającą jego identyfikację. Wykonawca załączając dokument oznacza, czy stanowi „tajemnicę przedsiębiorstwa” lub czy jest dokumentem „Jawnym” – niestanowiący tajemnicy przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Po uzupełnieniu niezbędnych pozycji i dodaniu załączników, wykonawca w celu złożenia oferty wybiera polecenie „Złóż ofertę/wniosek”. Następnie wykonawca potwierdza, że zapoznał się z dokumentami postępowania i chce złożyć ofertę. Potwierdzając chęć złożenia oferty wykonawca przechodzi do etapu podpisania oferty kwalifikowanym podpisem elektronicznym, w Systemie

automatycznie uruchomi się aplikacja do złożenia podpisu, w tym momencie wykonawca ma także podgląd do treści swojej oferty. Naciśnięcie polecenia „podpisz” oznacza podpisanie oferty przez Wykonawcę. Wykonawca ma także możliwość podpisania oferty poza Platformą, w tym celu należy użyć polecenia „Wygeneruj raport” co umożliwi pobranie oferty na dysk. Użycie polecenia „Zapisz” umożliwia zapisanie dotychczas uzupełnionych informacji i dodanych załączników, jedynie polecenie „Złóż ofertę/wniosek” prowadzi do skutecznego złożenia oferty w postępowaniu. Potwierdzeniem prawidłowo złożonej Oferty jest komunikat systemowy „Oferta złożona poprawie”.

8. Złożenie oferty wraz z dokumentami w postaci elektronicznej zapisanej na nośniku danych (np. CD, pendrive) jest niedopuszczalne, gdyż w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, forma ta nie jest uznawana jako złożenie przy użyciu środków komunikacji elektronicznej.
9. Możliwość otwarcia plików zawierających ofertę dostępna jest dopiero po upływie terminu składania ofert.
10. Wykonawcy ubiegający się wspólnie o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Stosowne pełnomocnictwo powinno być dołączone do oferty w oryginale lub kopii poświadczonej za zgodność z oryginałem notarialnie.

XVII. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

Ofertę należy złożyć do **28 lipca 2020 r. do godz. 12:00**

Ofertę **w formie papierowej** należy złożyć we wskazanym powyżej terminie w Kancelarii Ogólnej UP RP w Warszawie, pokój nr 9, al. Niepodległości 188/192.

Ofertę **w formie elektronicznej** należy złożyć we wskazanym powyżej terminie w sposób opisany w pkt XIII lit. B

Otwarcie ofert nastąpi **28 lipca 2020 r. o godz. 12:30 w pokoju nr 205** w siedzibie Zamawiającego.

Otwarcie ofert elektronicznych nastąpi przez upublicznienie wczytanych w Systemie (Platformie zakupowej). Otwarcie ofert jest jawne.

Niezwłocznie po otwarciu ofert Zamawiający zamieści w Systemie oraz na stronie internetowej informacje z otwarcia ofert zawierające elementy, o których mowa w art. 86 ust. 5 ustawy Pzp.

XVIII. OPIS SPOSOBU OBLICZENIA CENY

1. Wykonawca poda cenę za wykonanie zamówienia w Formularzu ofertowym (stanowiącym Załącznik nr 2 do SIWZ).
2. Podana cena musi obejmować wszystkie koszty realizacji prac z uwzględnieniem wszystkich opłat i podatków (także od towarów i usług). Cena oferty musi być podana w złotych polskich, cyfrowo do dwóch miejsc po przecinku oraz słownie.
3. Wszystkie ceny określone przez Wykonawcę zostaną ustalone na okres obowiązywania umowy i nie będą podlegały zmianom.

XIX. INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Rozliczenia między Zamawiającym a wykonawcą prowadzone będą w złotych polskich.

XX OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

Przy wyborze najkorzystniejszej oferty na każdą z części zamówienia Zamawiający będzie się kierował następującymi kryteriami:

Kryterium	Waga w %
Cena oferty brutto	60
Termin realizacji	40

1) Cena brutto oferty za realizację całego zamówienia (Pc) – wg wzoru

$$Pc = 60 \times (Cena\ min/C) [pkt]$$

gdzie:

- Pc - liczba punktów przyznanych ofercie w kryterium „Cena”,
Cena min - najniższa cena oferty brutto spośród ofert podlegających ocenie,
C - cena brutto ocenianej oferty.

Dla kryterium „Cena” przyjmuje się, że 1 % = 1 pkt i tak zostanie przeliczona liczba punktów. Maksymalna liczba punktów do uzyskania w tym kryterium wynosi 60 pkt. Punktacja będzie liczona z dokładnością do dwóch miejsc po przecinku.

2) Termin realizacji (Pt)

Termin realizacji

Przez „Termin realizacji” Zamawiający rozumie termin w którym Wykonawca dostarczy przedmiot zamówienia Zamawiającemu liczony w dniach roboczych:

Termin realizacji w dniach roboczych	Liczba punktów
Do 7 dni roboczych	40
Do 10 dni roboczych	20
Do 12 dni roboczych	0

Oferta z terminem dłuższym niż 12 dni zostanie odrzucona na podstawie art. 89 ust. 1 pkt 2 Ustawy jako oferta, której treść nie odpowiada treści specyfikacji istotnych warunków zamówienia.

Łączna ocena punktowa (P) będzie stanowiła sumę punktów uzyskanych we wszystkich wyżej wymienionych kryteriach i zostanie obliczona zgodnie z poniższym wzorem

$$P = Pc + Pt$$

gdzie:

- P - łączna ocena punktów przyznana ofercie,

- Pc - liczba punktów przyznanych ofercie w kryterium „Cena”,
Pt - liczba punktów przyznanych ofercie w kryterium „Termin realizacji”

Za najkorzystniejszą zostanie uznana oferta, która uzyska łącznie najwyższą liczbę punktów.

XXI. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

Miejsce i termin podpisania umowy zostanie uzgodniony telefonicznie lub pocztą elektroniczną pomiędzy Zamawiającym a Wykonawcą, którego oferta zostanie wybrana.

XXII. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia.

XXIII. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, OGÓLNE WARUNKI UMOWY ALBO WZÓR UMOWY, JEŻELI ZAMAWIAJĄCY WYMAGA OD WYKONAWCY, ABY ZAWARŁ Z NIM UMOWĘ W SPRAWIE ZAMÓWIENIA PUBLICZNEGO NA TAKICH WARUNKACH

UMOWA Nr/2020

podpisana w Warszawie dnia roku pomiędzy:

1/ Skarbem Państwa - Urzędem Patentowym Rzeczypospolitej Polskiej z siedzibą w Warszawie przy Al. Niepodległości 188/192, NIP 526-10-48-480, REGON 000332251, reprezentowanym przez:

..... – Dyrektora Generalnego,

zwanym w dalszej części umowy „**Zamawiającym**”

a

2/ z siedzibą w, posiadającą NIP i REGON, reprezentowaną przez:

zwaną w dalszej części umowy „**Wykonawcą**”

Wydruk informacji odpowiadającej odpisowi aktualnemu z stanowi załącznik nr 1.

Umowa została zawarta w wyniku przeprowadzonego postępowania w trybie przetargu nieograniczonego na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity Dz. U. z 2019 r., poz. 1843 z późn.zm.).

Termin	Definicja
Umowa	Umowa w sprawie zamówienia publicznego zawarta między Zamawiającym, a Wykonawcą wraz ze wszystkimi aneksami i załącznikami do Umowy.
Strona	Zamawiający lub Wykonawca, w zależności od kontekstu
Strony	Łącznie: Zamawiający i Wykonawca.
Aktualizacja	Uaktualnienie danej wersji Oprogramowania.
Dzień roboczy	dzień, który nie jest dniem ustawowo wolnym od pracy (od poniedziałku do piątku z wyłączeniem sobót, niedziel i określonych ustawą świąt).

§ 1.

Przedmiot umowy

1. Przedmiotem niniejszej umowy jest:
 - a) świadczenie usługi wsparcia producenta dla systemu antywirusowego Symantec Endpoint Protection (dla łącznie 900 licencji) zwanego dalej „Systemem”,
 - b) rozbudowa obecnego System (750 licencji) poprzez dostarczenie dodatkowych 150 licencji zapewniających ochronę antywirusową serwerów i stacji roboczych wraz ze wsparciem producenta dla całego Systemu(900 licencji), do dnia 1.08.2023 r. ,
 - c) przeprowadzenie przeglądu optymalizującego System,
 - d) udzielenie licencji na oprogramowanie i przeniesienie praw autorskich do dokumentacji: raportu z przeprowadzonego audytu i procedury upgradów dla serwerów .
2. Szczegółowy opis przedmiotu zamówienia określa załącznik Nr 2 do umowy.

§ 2.

Termin realizacji przedmiotu Umowy

1. Wykonawca zobowiązuje się do świadczenie usługi wsparcia producenta dla Systemu (Symantec Endpoint Protection łącznie dla 900 licencji) do dnia 1.08.2023 r.
2. Wykonawca zobowiązuje się do rozbudowy Systemu o dodatkowe 150 licencji oraz dostarczenia numeru umowy serwisowej producenta a także do wykonania przeglądu optymalizującego Systemu w terminie..... Dni roboczych od dnia zawarcia umowy („Termin realizacji”) [do uzupełnienia na podstawie oferty].

§ 3.

Sposób realizacji przedmiotu Umowy

1. W terminie do 10 Dni roboczych od zawarcia Umowy Wykonawca zobowiązuje się do przeglądu optymalizującego System, zawierającego w szczególności:
 - 1.1 Przegląd stanu konfiguracji środowiska;
 - 1.2 Przegląd i analizę konfiguracji polityk bezpieczeństwa poszczególnych modułów;
 - 1.3 Analizę, optymalizację i zalecenia dotyczące konfiguracji polityk bezpieczeństwa;
 - 1.4 Analizę błędów w działaniu środowiska i zalecenia dotyczące ich rozwiązania;
 - 1.5 Analizę i optymalizację systemowego raportowania automatycznego;
 - 1.6 Opracowanie procedury upgrade dla serwerów pracujących w trybie HA;

- 1.7 Raport z przeprowadzonego audytu wraz z zaleceniami dotyczącymi zmian konfiguracyjnych w funkcjonującym środowisku.
 2. Wykonawca przeprowadzi przegląd i przekaże raport w terminie 3 Dni roboczych od momentu jego rozpoczęcia.
 3. W ramach Umowy Zamawiający otrzymuje wsparcie techniczne producenta Systemu do dnia 1.08.2023 r. zapewniające:
 - 1.1 nieograniczoną ilość zgłoszeń serwisowych;
 - 1.2 nielimitowane wsparcie techniczne producenta drogą mailową i systemem zdalnej pomocy w Dni robocze w godzinach od 9.00 do 17.00, a w przypadku niemożności świadczenia usług wsparcia zdalnie wsparcie techniczne świadczone w siedzibie klienta z czasem reakcji na następny Dzień roboczy bez dodatkowych opłat;
 - 1.3 możliwość Aktualizacji głównej wersji oprogramowania;
 - 1.4 dostęp do portalu internetowego umożliwiającego pobieranie poprzednich wersji oprogramowania (jeśli producent oficjalnie wspiera poprzednie wersje), pobieranie nowych wersji oprogramowania lub poprawek (jeśli producent opublikuje nowe wersje lub poprawki w czasie trwającej usługi wsparcia);
 - 1.5 dostęp do materiałów producenta takich jak: dokumentacja techniczna (jeśli producent udostępnia dokumentację techniczną), internetowa baza wiedzy (jeśli producent oprogramowania udostępnia bazę wiedzy), forum internetowe producenta oprogramowania (jeśli producent oprogramowania udostępnia takie forum).
 4. Strony zgodnie oświadczają, że za datę wykonania przedmiotu umowy przyjmuje się podpisanie protokołu odbioru bez zastrzeżeń. Wzór protokołu odbioru zawiera załącznik Nr 3 do Umowy
5. Wykonawca odpowiada wobec Zamawiającego za wszelkie działania lub zaniechania Podwykonawców, jak za własne działania lub zaniechania.
6. Strony zobowiązują się do wzajemnego przekazywania sobie niezwłocznie wszelkich informacji mogących mieć wpływ na realizację Umowy. Wykonawca niezwłocznie udzieli odpowiedzi w formie pisemnej na zgłaszane przez Zamawiającego uwagi dotyczące realizacji przedmiotu Umowy, w terminie nie dłuższym niż 2 dni.

§ 4.

Oświadczenia Wykonawcy

1. Wykonawca oświadcza, że posiada wiedzę fachową i dysponuje wszelkimi niezbędnymi informacjami oraz pozwoleniami wymaganymi przez przepisy prawa w dziedzinach związanych z wykonaniem przedmiotu Umowy, a także dysponuje odpowiednim personelem i odpowiednimi środkami gwarantującymi profesjonalną realizację niniejszej Umowy.
2. Wykonawca oświadcza, że przedmiot Umowy nie jest obciążony prawem obligacyjnym ani rzeczowym na rzecz osób trzecich, nie toczy się wobec niego postępowanie egzekucyjne, sądowe, ani przed jakimkolwiek organem orzekającym oraz nie jest przedmiotem zabezpieczenia. Wykonawca oświadcza także, że brak jest jakichkolwiek innych okoliczności mogących ograniczyć prawa Zamawiającego wynikające z niniejszej Umowy.
3. Wykonawca oświadcza, że przysługują mu w zakresie wykonywania niniejszej Umowy wszelkie niezbędne prawa do sprzedaży oprogramowania/udzielenia licencji.
4. Wykonawca oświadcza, że wykonanie niniejszej Umowy nie będzie prowadzić do wypełnienia przesłanek czynu nieuczciwej konkurencji, w szczególności nie stanowi naruszenia tajemnicy przedsiębiorstwa osoby trzeciej.

§ 5.

Przedstawiciele Stron

1. Do bieżącej współpracy, w zakresie wykonywania niniejszej Umowy, upoważnione są następujące osoby:
 - 1.1. Po stronie Zamawiającego:
 - 1.1.1.
 - 1.1.2.lub inne wskazane przez Zamawiającego.
 - 1.2. Po stronie Wykonawcy:
 - 1.2.1.lub inne wskazane przez Wykonawcę.
2. Osoby wskazane w ust. 1 są upoważnione do wykonywania w imieniu Stron czynności określonych w niniejszej Umowie, z wyłączeniem zmiany postanowień tej Umowy, jej rozwiązania lub odstąpienia od niej.
3. Do uzgodnień i czynności wynikających lub mogących wynikać w związku z wykonaniem niniejszej Umowy oraz nadzoru nad jej realizacją Zamawiający upoważnia Dyrektora oraz Zastępcę Dyrektora Departamentu Informatyki.
4. Zmiana osób upoważnionych do dokonywania uzgodnień w trakcie realizacji Umowy wymaga poinformowania drugiej Strony na piśmie i nie stanowi zmiany Umowy.
5. Strony zobowiązują się do kierowania wszelkiej korespondencji wymagającej formy pisemnej na adresy stron wymienione w komparycji umowy, a w przypadku zmiany adresu, do niezwłocznego, pisemnego powiadomienia o tym fakcie drugiej Strony.
6. W przypadku braku powiadomienia, o którym mowa w ust. 5 niniejszego paragrafu doręczenie korespondencji na adres, o którym mowa w ust. 5 niniejszego paragrafu, wywiera przewidziane prawem skutki prawne.

§ 6.

Licencje na oprogramowanie, autorskie prawa majątkowe

1. Z chwilą podpisania protokołu odbioru w ramach wynagrodzenia, o którym mowa w § 7 ust. 1 Wykonawca zapewnia Zamawiającemu bezterminowe, bez ograniczeń terytorialnych prawo do korzystania z licencji na oprogramowania, o którym mowa w § 1 na następujących polach eksploatacji:
 - 1.1. korzystania z oprogramowania w ramach wszystkich funkcjonalności w dowolny sposób w liczbie zgodnej z § 1 ust. 1,
 - 1.2. wprowadzanie i zapisywanie w pamięci komputerów,
 - 1.3. odtwarzanie,
 - 1.4. utrwalanie,
 - 1.5. przekazywanie,
 - 1.6. przechowywanie,
 - 1.7. wyświetlanie,
 - 1.8. stosowanie,
 - 1.9. instalowanie i deinstalowanie oprogramowania pod warunkiem zachowania liczby udzielonych licencji,
 - 1.10. sporządzanie kopii zapasowej (kopii bezpieczeństwa) zainstalowanego oprogramowania,

2. Wykonawca oświadcza, że dostarczone przez niego oprogramowanie, nie narusza żadnych praw osób trzecich, zwłaszcza w zakresie własności przemysłowej, praw autorskich i praw pokrewnych oraz nieuczciwej konkurencji, i że posiada prawo do sprzedaży/udzielania licencji na oprogramowanie, które Wykonawca dostarczył, zgodnie z postanowieniami § 1 i przejmuje w tym zakresie odpowiedzialność w przypadku roszczeń osób trzecich.
3. Wykonawca oświadcza, że Aktualizacja oprogramowania, nie powoduje zmian w zakresie uprawnień, w tym pól eksploatacji uzyskanych przez Zamawiającego na podstawie niniejszej Umowy.
4. Wykonawca zobowiązuje się przenieść na Zamawiającego autorskie prawa majątkowe do dokumentacji stworzonej w wyniku wykonania zobowiązań wynikających z Umowy. Przeniesienie praw obejmuje następujące pola eksploatacji:
 - 1) trwałe lub czasowe zwielokrotnianie dokumentacji w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, w tym także utrwalanie i zwielokrotnianie takiej dokumentacji dowolną techniką, w tym techniką zapisu magnetycznego lub techniką cyfrową, taką jak zapis na płycie CD, DVD, Blu-ray, urządzeniu z pamięcią flash lub jakimkolwiek innym nośniku pamięci;
 - 2) obrót dokumentacją, w tym wprowadzanie do obrotu, użyczanie lub najem dokumentacji, a także rozpowszechnianie dokumentacji w inny sposób, w tym jej publiczne wykonywanie, wystawianie, wyświetlanie, odtwarzanie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.
5. Wykonawca zobowiązuje się przenieść na Zamawiającego:
 - 1) prawo zezwalania na wykonywanie zależnych praw autorskich do wszelkich opracowań dokumentacji (lub jej poszczególnych elementów), tj. prawo zezwalania na rozporządzanie i korzystanie z takich opracowań na polach eksploatacji wskazanych powyżej;
 - 2) własność wydanych Zamawiającemu nośników, na których została utrwalona dokumentacja (lub jej poszczególne elementy) w celu ich przekazania Zamawiającemu, z chwilą wydania tych nośników Zamawiającemu.
6. Przeniesienie przez Wykonawcę na Zamawiającego praw do dokumentacji, o których mowa powyżej nastąpi z chwilą podpisania protokołu odbioru.

§ 7.

Wynagrodzenie i warunki płatności

1. Za prawidłowe wykonanie Przedmiotu umowy Wykonawca otrzyma, zgodnie ze złożoną ofertą, wynagrodzenie w wysokości zł brutto (słownie: groszy), obejmujące również wszelkie obciążenia związane z realizacją Umowy, w tym wynagrodzenie za zapewnienie prawa do korzystania z oprogramowania przez Zamawiającego na określonych w niniejszej umowie polach eksploatacji, jak również wszystkie koszty, opłaty, wydatki Wykonawcy, a także podatki, w tym 23 % podatek od towarów i usług (VAT), w tym:
 - 1) Świadczenie usługi wsparcia i przeprowadzony audyt w kwocie: zł (słownie: zł);
 - 2) Dostawa i udzielenie 150 licencji w kwocie: zł (słownie: zł);
 - 3) Przeniesienie praw autorskich do dokumentacji powstałej w trakcie realizacji Umowy w kwocie: zł (słownie: zł).
2. Podstawą wystawienia faktury jest podpisany przez Strony bez zastrzeżeń Protokół odbioru.

3. Wypłata wynagrodzenia, o którym mowa w ust. 1, nastąpi przelewem w terminie 14 dni od dnia dostarczenia przez Wykonawcę do siedziby Zamawiającego prawidłowo wystawionej faktury na numer rachunku bankowego wskazany w fakturze. Wykonawca oświadcza, że rachunek, który będzie wskazany na fakturze został otwarty w związku z prowadzoną przez Wykonawcę działalnością gospodarczą, zgłoszony i ujawniony w wykazie prowadzonym przez Szefa Krajowej Administracji Skarbowej. Fakturę należy doręczyć Zamawiającemu na adres: al. Niepodległości 188/192, 00-950 Warszawa.
4. Za dzień zapłaty wynagrodzenia uznaje się dzień obciążenia rachunku bankowego Zamawiającego.

§ 8.

Kary umowne

1. W przypadku odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % wartości Umowy brutto.
2. W przypadku odstąpienia od Umowy przez Wykonawcę z przyczyn leżących po jego stronie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % wartości Umowy brutto.
3. W przypadku opóźnienia terminu, o którym mowa w § 2 ust. 2 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500 zł za każdy rozpoczęty Dzień roboczy opóźnienia terminu, chyba że przyczyny opóźnienia terminu leżą po stronie Zamawiającego.
4. W przypadku braku dostępności wsparcia o którym mowa w § 3 ust. 3 Umowy Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 100 zł za każdy rozpoczęty Dzień roboczy braku dostępności wsparcia.
5. Kary umowne przewidziane w niniejszym paragrafie obowiązują niezależnie od siebie, z tym zastrzeżeniem, że w przypadku odstąpienia od Umowy, możliwe jest naliczenie wyłącznie kary przewidzianej na wypadek odstąpienia od Umowy z tym, że w przypadku odstąpienia od części Umowy zastrzeżenie to dotyczy tylko części Umowy objętej odstąpieniem.
6. Zapłata przez Wykonawcę kar umownych z tytułu niewykonania lub nienależytego wykonania Umowy, nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego ustalone powyżej kary umowne na zasadach ogólnych.

§ 9.

Ochrona danych osobowych, klauzule informacyjne

1. Strony oświadczają, iż wszelkie dane osobowe pozyskane od siebie w związku z Umową przetwarzane będą przez Strony wyłącznie na potrzeby realizacji Umowy oraz chronione będą przed dostępem osób nieupoważnionych, zgodnie z obowiązującymi przepisami o ochronie danych osobowych: Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U z 2019 roku poz.1781).
2. W związku z udostępnianiem sobie wzajemnie przez Strony (administratorów danych) danych osobowych, Strony zamieszczają postanowienia określające jego zakres oraz wymagane informacje:
 - a) Dane osobowe osób reprezentujących każdą ze Stron wymienionych w części wstępnej Umowy oraz osób wyznaczonych do kontaktów i dokonywania bieżących uzgodnień oraz nadzoru nad realizacją umowy, a ponadto upoważnionych przez Wykonawcę do wystawienia faktury udostępniane będą drugiej Stronie i będą przetwarzane w celu realizacji Umowy (podstawa przetwarzania danych osobowych – art. 6 ust. 1 pkt b, pkt c, pkt e ogólnego rozporządzenia o ochronie danych).

b) Każda ze Stron oświadcza, że jej pracownicy wymienieni wyżej pod lit. a) w zakresie swoich obowiązków zostaną zaznajomieni z niniejszą Umową, w tym z zapisami zawartymi poniżej pod lit. c) i d).

c) Każda z osób wymienionych powyżej, pod lit. a), posiada prawo żądania dostępu do swoich danych osobowych, ich sprostowania oraz prawo wniesienia sprzeciwu wobec przetwarzania danych osobowych, a także prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w wypadku uznania, że administrator naruszył przepisy o ochronie danych osobowych. Dane będą ujawniane uprawnionym pracownikom Stron oraz podmiotom i ich pracownikom świadczącym usługi prawne, finansowe, księgowe i informatyczne.

d) Wykonawca podaje, że dane te będzie przetwarzał w okresie koniecznym do realizacji i rozliczenia Umowy z uwzględnieniem okresu przedawnienia oraz przepisów podatkowych oraz, iż powoła osobę odpowiedzialną (np. inspektora ochrony danych osobowych lub inną) z którą można będzie skontaktować się poprzez

Zamawiający podaje, że dane te będzie przetwarzał w okresie koniecznym do realizacji i rozliczenia Umowy, z uwzględnieniem okresu przedawnienia oraz przepisów podatkowych, oraz iż powoła inspektora ochrony danych, z którym można się będzie skontaktować poprzez adres email: iod@uprp.gov.pl lub pod numerem telefonu 22 579 00 25

§ 10.

Odstąpienie od umowy

1. Zamawiający może odstąpić od Umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. Zamawiający może odstąpić od umowy z przyczyn leżących po stronie Wykonawcy, gdy:
 - 2.1. Wykonawca opóźnia się w spełnieniu przedmiotu Umowy powyżej 7 dni;
 - 2.2. Wykonawca nienależycie wykonuje umowę, w szczególności nie stosuje się do uwag Zamawiającego lub narusza inne postanowienia Umowy i w przypadku gdy po upływie 7 dni od wezwania przez Zamawiającego do zaniechania przez Wykonawcę naruszeń postanowień Umowy i usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do wezwania.
3. Zamawiający może odstąpić od Umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. W tym przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu należytego wykonania części umowy.
4. Prawo odstąpienia Zamawiający może wykonać w terminie 30 dni od powzięcia wiadomości o okolicznościach, o których mowa w niniejszym paragrafie.
5. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności i wymaga uzasadnienia.
6. W przypadku odstąpienia od Umowy Zamawiający nie traci uprawnienia do naliczania należnych z tytułu odstąpienia od Umowy kar umownych.

§ 11.

Zmiany umowy

1. Wszelkie zmiany i uzupełnienia niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.

2. Zmiany Umowy nie stanowi w szczególności zmiana nazw/określeń Stron, siedziby Stron, numerów kont bankowych Stron, jak również osób odpowiedzialnych za realizację przedmiotu Umowy ze strony Wykonawcy oraz przedstawicieli Zamawiającego.

§ 12.

Postanowienia końcowe

1. W sprawach nieuregulowanych umową zastosowanie mają odpowiednie przepisy prawa, w szczególności ustawy Prawo zamówień publicznych, Kodeksu cywilnego, ustawy o prawie autorskim i prawach pokrewnych oraz ustawy o ochronie danych osobowych.
2. W przypadku rozbieżności interpretacyjnych pomiędzy postanowieniami umowy, a treścią załączników i innych dokumentów stanowiących integralną część Umowy lub wytworzonych przez Strony, pierwszeństwo mają postanowienia Umowy.
3. Wszystkie tytuły paragrafów w umowie mają charakter wyłącznie informacyjny i nie mają wpływu na interpretację postanowień Umowy.
4. Wykonawca nie może przenieść na osobę trzecią praw i obowiązków wynikających z Umowy, w całości lub w części.
5. Umowa podlega prawu polskiemu i zgodnie z nim powinna być interpretowana.
6. Strony umowy podejmą w dobrej wierze wysiłek w celu rozwiązania wszelkich sporów powstałych pomiędzy Stronami, które wynikły w związku z realizacją Umowy i/lub jej interpretacją. O ile rozwiązanie sporu nie powiedzie się, zostanie on poddany pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
7. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
8. Umowę sporządzono dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy.
9. Załączniki stanowiące integralną część umowy:
 - Załącznik Nr 1 - Wydruk informacji odpowiadającej odpisowi aktualnemu z..
 - Załącznik Nr 2 – Opis przedmiotu zamówienia
 - Załącznik Nr 3 - Protokół Odbioru

Zamawiający

.....
(imię i nazwisko, podpis)

Wykonawca

.....
(imię i nazwisko, podpis)

Protokół Odbioru

Warszawa, dnia / /

Na podstawie § 3 ust. 4 ww. Umowy dokonano odbioru Przedmiotu Umowy w postaci:

- rozbudowy Systemu o dodatkowe 150 licencji;
- odbioru numeru umowy serwisowej wsparcia producenta nr
- odbioru raportu z wykonanego przeglądu Systemu.

Przedmiot Umowy w zakresie objętym odbiorem został wykonany w terminie /nie został wykonany w terminie*

- | |
|--|
| 1. <u>Zgodnie z Umową wykonanie Przedmiotu Umowy objętego niniejszym odbiorem powinno nastąpić do dnia</u> |
| 2. <u>Faktyczne wykonanie Przedmiotu Umowy objętego niniejszym odbiorem nastąpiło w dniu</u> |

Przedmiot Umowy został odebrany bez zastrzeżeń / z zastrzeżeniami*.

UWAGI:

.....

Za Zamawiającego	Za Wykonawcę
..... (imię i nazwisko, podpis)	 (imię i nazwisko, podpis)

XXIV. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

1. Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp, przysługują środki ochrony prawnej określone w Dziale VI ustawy Pzp. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy Pzp.
2. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy Pzp czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie ustawy Pzp, wobec czynności:
 - 1) określenia warunków udziału w postępowaniu;
 - 2) wykluczenia odwołującego z postępowania o udzielenie zamówienia;
 - 3) odrzucenia oferty odwołującego;
 - 4) opisu przedmiotu zamówienia;
 - 5) wyboru najkorzystniejszej oferty.
1. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy Pzp, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
2. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo elektronicznej podpisane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub równoważnego środka, spełniającego wymagania dla tego rodzaju podpisu.
3. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Terminy wniesienia odwołania:
 - 1) Odwołanie wnosi się w terminie 5 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane w sposób określony w art. 180 ust. 5 zdanie drugie ustawy Pzp albo w terminie 10 dni - jeżeli zostały przesłane w inny sposób.
 - 2) Odwołanie wobec treści ogłoszenia o zamówieniu, a także wobec postanowień specyfikacji istotnych warunków zamówienia, wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub specyfikacji istotnych warunków zamówienia na stronie internetowej.
 - 3) Odwołanie wobec czynności innych niż określone w pkt 1 i 2 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
 - 4) Jeżeli Zamawiający nie przesłał Wykonawcy zawiadomienia o wyborze oferty

najkorzystniejszej odwołanie wnosi się nie później niż w terminie:

- a) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o udzieleniu zamówienia;
 - b) 1 miesiąca od dnia zawarcia umowy, jeżeli Zamawiający nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o udzieleniu zamówienia.
7. Szczegółowe zasady postępowania po wniesieniu odwołania, określają stosowne przepisy Działu VI ustawy Pzp.
8. Na orzeczenie Krajowej Izby Odwoławczej, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
9. Skargę wnosi się do sądu okręgowego właściwego dla siedziby Zamawiającego, za pośrednictwem Prezesa Krajowej Izby Odwoławczej w terminie 7 dni od dnia doręczenia orzeczenia Krajowej Izby Odwoławczej, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2012 r. poz. 1529) jest równoznaczne z jej wniesieniem.

XXV. MAKSYMALNĄ LICZBĘ WYKONAWCÓW, Z KTÓRYMI ZAMAWIAJĄCY ZAWRZE UMOWĘ RAMOWĄ, JEŚLI ZAMAWIAJĄCY PRZEWIDUJE ZAWARCIE UMOWY RAMOWEJ

Nie dotyczy.

XXVI. ADRES POCZTY ELEKTRONICZNEJ LUB STRONY INTERNETOWEJ ZAMAWIAJĄCEGO

Strona internetowa: <https://uprp.gov.pl>

Adres poczty elektronicznej: wzp1920@uprp.gov.pl

XXVII. WYSOKOŚĆ ZWROTU KOSZTÓW UDZIAŁU W POSTĘPOWANIU, JEŻELI ZAMAWIAJĄCY PRZEWIDUJE ICH ZWROT

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

XXVIII. KLAUZULA INFORMACYJNA ZGODNIE Z ART. 13 UST. 1 I 2 ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 Z DNIA 27 KWIETNIA 2016 W SPRAWIE OCHRONY OSÓB FIZYCZNYCH W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH I W SPRAWIE SWOBODNEGO PRZEPŁYWU TAKICH DANYCH ORAZ UCHYLENIA DYREKTYWY 95/46/WE (OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH) (DZ.URZ. UE L 119 Z 04.05.2016, STR 1), „RODO”

Na podstawie powołanych regulacji informuję, że:

- administratorem Pani/Pana danych osobowych jest Urząd Patentowy Rzeczypospolitej Polskiej 00-950 Warszawa, al. Niepodległości 188/192;
- kontakt do Inspektora ochrony danych - adres e-mailowy: iod@uprp.gov.pl, tel. 22 57 90 025, fax 22 57 90 001.
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO oraz ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2019 poz. 1843 ze zmian.) w celu związanym z postępowaniem o udzielenie zamówienia publicznego na

„Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu” prowadzonym w trybie przetargu nieograniczonego;

- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp;
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- posiada Pani/Pan:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych[1];
 - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO [2];
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
 - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

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

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

XXIX. POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w niniejszej specyfikacji mają zastosowanie przepisy ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843 ze zmian.), przepisy wykonawcze wydane na jej podstawie oraz przepisy kodeksu cywilnego.

ZAŁĄCZNIKI DO SIWZ

1. Opis przedmiotu zamówienia;
2. Formularz ofertowy (wzór);
3. Oświadczenie o braku podstawy do wykluczenia z postępowania (wzór)
4. Oświadczenie o spełnianiu warunków udziału w postępowaniu (wzór)
5. Oświadczenie dotyczące grupy kapitałowej.

OPIS PRZEDMIOTU ZAMÓWIENIA

Zamawiający eksploatuje obecnie **750 licencji SYMC ENDPOINT PROTECTION 14 PER USER RENEWAL BASIC 36 MONTHS GOV BAND A** ważnych do dnia **01.08.2020**.

Ochroną objęte jest około 120 serwerów Windows, 170 serwerów Linux, pozostała pula licencja wykorzystana jest na komputery i laptopy głównie z OS Windows 10. Końcówki pracują zarówno w sieci Urzędu Patentowego jak i poza nią w trybie pracy zdalnej. Całość sterowana jest z poziomu jednego, własnego serwera dystrybucyjno-zarządczego SEP14.2.

Przedmiotem zamówienia jest zakup usługi wsparcia producenckiego dla działającego w Urzędzie Patentowym Rzeczypospolitej Polskiej systemu antywirusowego **Symantec Endpoint Protection** oraz **rozbudowa tego systemu do 900 licencji**, zapewniających jednoczesną ochronę antywirusową serwerów i stacji roboczych ważną do dnia co najmniej **01.08.2023** lub równoważne.

W ramach usługi wsparcia Wykonawca, w uzgodnionym z Zamawiającym terminie, przeprowadzi przegląd ukierunkowany na optymalizację konfiguracji dostarczanego systemu antywirusowego w poniższym zakresie:

- Przegląd stanu konfiguracji środowiska.
- Przegląd i analiza konfiguracji polityk bezpieczeństwa poszczególnych modułów.
- Analiza, optymalizacja i zalecenia dotyczące konfiguracji polityk bezpieczeństwa.
- Analiza błędów w działaniu środowiska i zalecenia dotyczące ich rozwiązania.
- Analiza i optymalizacja systemowego raportowania automatycznego.
- Opracowanie procedury upgrade dla serwerów pracujących w trybie HA.
- Raport z przeprowadzonego audytu wraz z zaleceniami dotyczącymi zmian konfiguracyjnych w funkcjonującym środowisku.

Maksymalny czas trwania przeglądu to trzy dni robocze.

I. Wymagania Zamawiającego:

1. Zamawiający wymaga od Wykonawcy, aby dostarczył technologie systemu antywirusowego zgodne z użytkowanym przez Zamawiającego systemem **Symantec Endpoint Protection**

Gwarancja i wsparcie dla dostarczanego oprogramowania

1. Dostarczone Oprogramowanie musi być objęte wsparciem technicznym producenta co najmniej do dnia 01.08.2023 (które może być realizowane także przez podmioty autoryzowane przez producenta),

2. Usługa wsparcia technicznego producenta oferowanego oprogramowania zapewniająca minimum:
- 1) nieograniczoną ilość zgłoszeń serwisowych;
 - 2) nielimitowane wsparcie techniczne drogą mailową i systemem zdalnej pomocy, a w przypadku niemożności świadczenia usług asysty technicznej zdalnie wsparcie techniczne świadczone w siedzibie klienta z czasem reakcji na następny dzień roboczy, bez dodatkowych opłat;
 - 3) dostęp do materiałów producenta takich jak: dokumentacja techniczna (jeśli producent udostępnia dokumentację techniczną), internetowa baza wiedzy (jeśli producent oprogramowania udostępnia bazę wiedzy), forum internetowe producenta oprogramowania (jeśli producent oprogramowania udostępnia takie forum);
 - 4) dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia, bez dodatkowych opłat;
 - 5) możliwość aktualizacji głównej wersji oprogramowania objętego usługą wsparcia, bez dodatkowych opłat;
 - 6) dostęp do portalu internetowego umożliwiającego: pobieranie poprzednich wersji oprogramowania (jeśli producent oficjalnie wspiera poprzednie wersje), pobieranie nowych wersji oprogramowania lub poprawek (jeśli producent opublikuje nowe wersje lub poprawki w czasie trwającej usługi wsparcia);
 - 7) oferowana usługa wsparcia producenta musi zapewniać ciągłość i poufność komunikacji na poszczególnych etapach procesowania zgłoszenia;
 - 8) wsparcie techniczne producenta musi być świadczone minimum w trybie 5x8: poniedziałek - piątek (5 dni w tygodniu) przez co najmniej 8 godzin dziennie;

II. Warunki równoważności

1. Jeżeli Zamawiający określił w SIWZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.
2. W przypadku dostarczania sprzętu, oprogramowania, szkoleń lub innych produktów równoważnych względem wyspecyfikowanych przez Zamawiającego w SIWZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane produkty spełniają wszystkie wymagania i warunki określone SIWZ, w szczególności w zakresie:
 - 1) warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które nie mogą być gorsze niż dla produktu wymienionego w SIWZ,
 - 2) funkcjonalności równoważnej produktu, która nie może być gorsza od funkcjonalności produktu wymienionego w SIWZ
 - 3) sprzętu i oprogramowania, które muszą być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego,
 - 4) sprzętu i oprogramowania, które nie mogą zakłócić pracy środowiska systemowo-programowego Zamawiającego,
 - 5) sprzętu i oprogramowania, które muszą w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
 - 6) sprzętu i oprogramowania, które muszą zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność produktu równoważnego z produktem określonym w SIWZ,

- 7) warunków i zakresu usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji produktu równoważnego, muszą być nie gorsze niż dla produktu wymienionego w SIWZ.,
3. W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego.
4. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty.
5. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo - programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego.
6. Wraz z produktem równoważnym Wykonawca jest zobowiązany do dostarczenia niżej wymienionego oświadczenia i następujących dokumentów:
 - 1) oświadczenia dotyczącego zastosowania produktu równoważnego,
 - 2) pełnego postanowienia licencji / sublicencji produktu równoważnego,
 - 3) pełnego wykazu funkcjonalności produktu równoważnego,
 - 4) pełnych warunków i zasad świadczenia usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji dla produktu równoważnego,
 - 5) wykazu miejsc użycia produktu równoważnego.
7. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.
8. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

III. Wymagania funkcjonalne dla oprogramowania antywirusowego

Oprogramowanie Antywirusowe i konsola zarządzająca, obsługująca w ramach jednego, spójnego systemu 900 jednocześnie działających urządzeń musi spełniać następujące wymagania:

Ochrona antywirusowa:

- Usuwanie wirusów, makro-wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware” i „adware”, włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu.

- Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym.
- Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie.
- Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane.
- Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych.
- Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:
 - a) na dyskach twardych
 - b) w boot sektorach
 - c) na dyskietkach
 - d) na płytach CD/DVD
 - e) na zewnętrznych nośnikach pamięci (np. podłączonych przez port USB).
- Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej.
- Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.
- Scentralizowaną obsługę wirusów polegającą na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań.
- Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek.
- Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, ARJ, RAR, MIME/UU, TAR, kontenery CAB,UUE, Rich Text Format.
- Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej.
- Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące.
- Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zestawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów.
- Możliwość natychmiastowego „wypchnięcia” definicji wirusów do stacji klienckich
- Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej trzy razy dziennie.
- Możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę.
- Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
- Dedykowany moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger – analiza zachowania opiera się na wykonywanych przez aplikację czynnościach (tworzenie nowych plików, komunikacja z internetem, podmiana strony w przeglądarce, itp.).
- Dedykowany moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą.
- Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.

- Automatyczne ponowne uruchomienie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.
- Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
- Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
- Skanowanie poczty klienckiej (na komputerze klienckim).
- Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach.
- Ściągnięcie dowolnego pliku na komputer musi spowodować sprawdzenie reputacji takiego pliku – jako reputacja rozumie się odpowiedź, co do ilości użytkowników w Internecie korzystających z danej aplikacji/pliku, czasu, kiedy aplikacja/plik pojawiła się w Internecie po raz pierwszy oraz czy aplikacja/plik jest „prawidłowa” czy też nie.
- Produkt musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikację, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 5, 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni.
- Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.
- Możliwość wyboru wielkości definicji antywirusowych, z której będzie korzystał zainstalowany agent – system musi posiadać pełną wersję sygnatur oraz ich wersję uproszczoną znacząco mniejszą o pełnej do instalacji na systemach z niewielką ilością miejsca na dyskach oraz w systemach VDI.

Zapora ogniowa – system Firewall:

- Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.
- Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.
- Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać.
- Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne.
- Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli.
- Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji.
- Konfiguracja stacji ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji DNS (FQDN) lub domeny DNS.
- Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.
- W przypadku wykrycia zdefiniowanego ruchu, firewall ma wysłać wiadomość do administratora.
- Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www.

- Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację.
- Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP
- Domyślne reguły zezwalające na ruch DHCP, DNS, WINS.

Ochrona przed włamaniami – system IPS:

- Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie.
- Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.
- Produkt ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur). Sygnatury te mogą działać w trybie blokuj lub rejestruj.
- Wykrywanie skanowania portów.
- Ochrona przed atakami typu odmowa usług (Denial of Service).
- Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC).
- Wykrywanie trojanów i generowanego przez nie ruchu.
- Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.
- Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków.
- System ochrony przed włamaniami musi automatycznie integrować się z przeglądarką internetową (przynajmniej z Internet Explorer oraz Firefox) – uniemożliwiając wykonanie w nich (nawet, jeżeli są podatne) szkodliwego dla nich kodu.

Ochrona systemu operacyjnego:

- Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji.
- Produkt ma umożliwiać ładowanie modułów lub bibliotek DLL.
- Produkt ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje.
- Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową.
- Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika.
- Produkt ma kontrolować dostęp do rejestru systemowego.
- Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne.
- Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych.
- Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu.
- Możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego.
- Możliwość utworzenia listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, by żadna inna aplikacja/biblioteka z poza listy nie mogła uruchomić się na komputerze.

- Kolekcja aktualnie znajdujących się aplikacji na systemie końcowym musi być możliwa do wywołania bezpośrednio z konsoli zarządzającej – bez konieczności wykonania jakichkolwiek czynności na systemie końcowym.
- Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, by tylko aplikacja znajdujące się na liście nie mogły uruchomić się na komputerze.
- Możliwość automatycznego importu list zarówno białej, jak i czarnej, co zdefiniowany interwał czasu.

Integralności komputera:

- Oprogramowanie musi umożliwiać wykonywanie szerokiego zakresu testów integralności komputera pod kątem zgodności z polityką bezpieczeństwa urządzeń końcowych, w tym: programów antywirusowych, poprawki firmy Microsoft, dodatki Service Pack firmy Microsoft, osobistych zapór ogniowych.
- Testy integralności mają być przeprowadzane cyklicznie, co zdefiniowany okres czasu.
- Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta.
- Oprogramowanie musi umożliwiać wykonanie niestandardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać zaawansowaną składnię If...Then...Else.
- W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:
 - a) Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne
 - b) Pliki - istnienie, data, rozmiar, suma kontrolna
 - c) Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego
 - d) Zainstalowane poprawki
 - e) Uruchomiony proces, wersja systemu operacyjnego
 - f) Własna aplikacja
- W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako możliwe operacje do wykonania, musi istnieć możliwość:
 - Uruchamianie dowolnego/własnego skryptu lub programu
 - Logowanie zdarzenia
 - Ukazanie okienka z wiadomością
 - Pobieranie oraz uruchamianie instalacji
 - Ma istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.
 - Możliwość wymuszenia instalacji dowolnej aplikacji.
- W wypadku niezgodności własnego systemu, oprogramowanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.
- Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.
- Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.

- Musi istnieć test integralności komputera, który sprawdzi czy komputer nie jest podłączony do Internetu poprzez dwie różne drogi, np. poprzez kabel sieciowy (Ethernet) i poprzez dostęp mobilny (WiFi, modem GSM, etc.)

Ochrona środowisk wirtualnych:

- Produkt musi umożliwiać identyfikację środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Microsoft Hyper-V, VMWare.
- Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym.
- Produkt musi umożliwiać prawidłowe rozliczenia licencji oferowanego systemu dla systemów wirtualnych typu desktop tzw. VDI, w szczególności tzw. „non-persistent”.
- Produkt musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń.

Architektura:

- Rozwiązanie ma mieć architekturę trój-warstwową. Klienci mają być zarządzani przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez konsolę administratora.
- Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.
- Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.
- Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.
- Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.
- Serwery zarządzające mają móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).
- Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostawcy aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.
- Definiowanie lokalnego repozytorium musi zawierać warunki, jakie muszą być zachowane by dany komputer mógł stać się lokalnym repozytorium – warunkami muszą być przynajmniej: wersja systemu operacyjnego, adres komputera, nazwa komputera (z możliwością podania ją ze znakami specjalnymi, np.: komputer*), określonego wpisu w rejestrze.
- Możliwość manualnego wskazania wybranej grupie komputerów konkretnego lokalnego dostawcy aktualizacji.
- Możliwość ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.

Moduł raportujący:

- Produkt ma zapewniać graficzne raportowanie.
- Wbudowane raporty mają pokazywać:

- a) stan dystrybucji sygnatur antywirusowych, sygnatur heurystycznych oraz IDS/IPS
 - b) wersje zainstalowanych klientów
 - c) inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor)
 - d) wykrytych wirusów, zdarzeń sieciowych, integralności komputerów
 - e) zainstalowane technologie i ich aktualny stan
- Moduł raportowania ma pokazywać stan wykonywanych poleceń na komputerach.
 - Możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych.
 - Produkt musi umożliwiać automatyczne zbudowanie zapytań, które będą wykonywane o zdanym czasie i ich wynik będzie przechowywany w postaci kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwijanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór interesujących danych). Wszystkie te operacje muszą być wykonywane graficznie.
 - Produkt musi umożliwiać automatyczne budowanie trendów.
 - Produkt musi umożliwiać automatyczne budowanie kluczowych wskaźników wydajności (KPI).

Moduł centralnego zarządzania:

- Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z konsoli.
- Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci.
- Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.
- Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.
- Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami.
- Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.
- Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.
- Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.
- Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.
- Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.
- Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.
- Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.
- Lokalizacja ma być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.

- Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I” oraz „LUB” na powyżej wymienionych elementach.
- Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji.
- W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu.
- Nowe wersje oprogramowania mają być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.
- Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.
- Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia:
 - a) błędnej autoryzacji do systemu zarządzania
 - b) dostępności nowego oprogramowania
 - c) pojawienia się nowego komputera
 - d) zdarzeń powiązanych z infekcjami wirusów
 - e) stanu serwerów zarządzających
- Możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji.
- Oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający.
- Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

Platforma:

- Oprogramowanie musi działać na systemach Windows XP 32/64-bit, Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8/8.1 32/64-bit, Windows 10 32/64-bit, Windows Server 2003 32/64-bit, Windows Server 2008 32/64-bit, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.
- Komponenty rozwiązania takie jak: firewall, zapobieganie włamaniom, kontrola urządzeń i aplikacji oraz kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.
- Serwer zarządzający musi działać na systemach Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.

Ochrona antywirusowa dla systemu Macintosh:

- Ochrona antywirusowa (z pominięciem funkcji reputacji) oraz system IPS ma działać na platformie Mac OS.
- Klient dla systemu Mac ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.

Ochrona antywirusowa dla systemu Linux:

- Ochrona antywirusowa z pominięciem funkcji reputacji ma działać na platformie CentOS 6.x, 7.x, SuSE Linux Enterprise (server/desktop) 10.x, 11.x, Oracle Linux 5.x, 6.x, Ubuntu 8.x-14.x, 11.x, Debian 5.x, 6.x, 7x, RedHat 7.5.

- Klient dla system Linux ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.

Opis prac instalacyjnych w przypadku systemów równoważnych:

- Wykonawca w terminie 2 dni od podpisania umowy przygotowuje i przedstawi do akceptacji Zamawiającego harmonogram realizacji umowy.
- Instalacja oraz konfiguracja środowiska oraz polityk bezpieczeństwa będzie odbywać się na podstawie zatwierdzonego harmonogramu.
- **Zamawiający posiada obecnie system antywirusowy Symantec Endpoint Protection wraz z konsolą zarządzającą Symantec Endpoint Protection Manager dla 750 jednocześnie działających urządzeń.** Wykonawca odinstaluje obecnie używane oprogramowanie antywirusowe dla grupy aktywnych urządzeń z systemami operacyjnymi: Microsoft Windows XP/7/10, Windows Server 2003/2008 R2/2012 R2/2016/2019, Linux RedHat7.5, MacOS
- Wykonawca przeprowadzi dystrybucję wdrażanego oprogramowania antywirusowego dla grupy 900 aktywnych urządzeń z systemami operacyjnymi: Microsoft Windows XP/7/10, Windows Server 2003/2008 R2/2012 R2/2016/2019, Linux RedHat7.5, MacOS.
- Po wykonaniu wszystkich prac Wykonawca opracuje szczegółową dokumentację powykonawczą.

.....
Pieczęć Wykonawcy

FORMULARZ OFERTOWY

Nazwa i adres Wykonawcy:

.....

.....

Wykonawca należy do MSP: *(należy zaznaczyć właściwe)* Tak / Nie

Nawiązując do postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego (nr BG-II.211.19.2020) pn. „**Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu**”

w imieniu reprezentowanego przeze mnie/przez nas Wykonawcy:

1. Oferujemy wykonanie przedmiotu zamówienia w zakresie objętym SIWZ oraz z uwzględnieniem wszystkich elementów określonych w opisie przedmiotu zamówienia za łączną:

cenę brutto (łącznie z podatkiem VAT)zł

(słownie złotych:).

w tym:

- 1) Świadczenie usługi wsparcia i przeprowadzony audyt w kwocie: zł
- 2) Dostawa i udzielenie 150 licencji w kwocie: zł
- 3) Przeniesienie praw autorskich do dokumentacji powstałej w trakcie realizacji umowy w kwocie: zł
2. Oferujemy **dniowy termin realizacji przedmiotu zamówienia** *(nie może być dłuższy niż 12 dni)*.
3. Akceptujemy zapłatę należności zgodnie z warunkami zawartymi w § 7 istotnych postanowień umowy.
4. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
5. Oświadczamy, że zapoznaliśmy się z postanowieniami umowy, które stanowią punkt XXIII Specyfikacji Istotnych Warunków Zamówienia i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na określonych w tym punkcie warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.

6. Uważamy się za związanych niniejszą ofertą na czas wskazany w SIWZ, czyli przez okres 30 dni od upływu terminu składania ofert.
7. Oświadczamy, że usługi, które będziemy świadczyć nie są obciążone prawami osób trzecich.
8. Następującą część zamówienia powierzamy do wykonania podwykonawcy* (*wypełnić jeżeli taka część występuje)

L.p.	Część zamówienia powierzona do wykonania Podwykonawcy	Nazwa/firma Podwykonawcy oraz jego adres

9. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na nasz adres:

.....

Imię i nazwisko osoby do kontaktu:.....

tel..... faks e-mail.....

10. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO - wykonawca nie składa powołanego oświadczenia (treść oświadczenia z punktu 10 należy wtedy przekreślić).

11. Oferta niniejsza wraz z załącznikami składa się zkolejno ponumerowanych kartek.

Załącznikami do niniejszej oferty, stanowiącymi jej integralną część są:

1.
2.

 (miejscowość, data)

 (imię i nazwisko oraz podpis
 upoważnionego przedstawiciela/przedstawicieli
 Wykonawcy)

**OŚWIADCZENIE
O NIEPODLEGANIU WYKLUCZENIU**

Składając ofertę w postępowaniu nr BG-II.211.19.2020 o udzielenie zamówienia publicznego, prowadzonym w trybie przetargu nieograniczonego pn.:

„Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu”

W IMIENIU WYKONAWCY:

.....
/wpisać nazwę (firmę) Wykonawcy/

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-23 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.

..... (miejscowość), dnia r.

.....
(podpis)

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

.....

..... (miejscowość), dnia r.

.....
(podpis)

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.:

.....

/wpisać nazwę (firmę) Podmiotu/ów

nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

..... (miejscowość), dnia r.

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, będącego/ych Podwykonawcą/ami:

.....

/wpisać nazwę (firmę) Podwykonawcy/ów

nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

..... (miejscowość), dnia r.

.....

(podpis)

**OŚWIADCZENIE
O SPEŁNIANIU WARUNKÓW UDZIAŁU
W POSTĘPOWANIU**

Składając ofertę w postępowaniu nr BG-II.211.19.2020 o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego pn.:

„Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu”

W IMIENIU WYKONAWCY:

.....

/wpisać nazwę (firmę) Wykonawcy/

Oświadczam/y, że spełniam/y warunki udziału w postępowaniu.

.....dnia

.....

(podpis Wykonawcy/Pełnomocnika)

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, polegam na zasobach następującego/ych podmiotu/ów:

.....

w następującym zakresie:

.....

.....dnia

.....

(podpis Wykonawcy/Pełnomocnika)

.....
Pieczęć Wykonawcy

OŚWIADCZENIE
o przynależności lub braku przynależności do grupy kapitałowej,
o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp

Przystępując do postępowania o udzielenie zamówienia publicznego, prowadzonego w trybie przetargu nieograniczonego pn.: „**Wsparcie producenckie dla systemu antywirusowego oraz rozbudowa tego systemu**” (nr post. BG-II.211.19.2020) oświadczam, że na dzień składania ofert reprezentowany przeze mnie/przez nas Wykonawca:

☐ **nie należy do grupy kapitałowej¹** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634).

☐ **należy do grupy kapitałowej¹** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), w której skład wchodzi następujące podmioty (podać nazwę i siedzibę):

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

Niniejsze oświadczenie składam/składamy, pod rygorem wykluczenia z postępowania w przypadku złożenia odrębnych ofert, oferty częściowej lub wniosku o dopuszczenie do udziału w tym postępowaniu przez Wykonawców należących do tej samej grupy kapitałowej, w rozumieniu ww. ustawy (chyba że zostanie wykazane, że istniejące między podmiotami powiązania w ramach grupy kapitałowej nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia).

*** właściwe zaznaczyć znakiem X**

(miejscowość, data)

(imię i nazwisko oraz podpis upoważnionego przedstawiciela/przedstawicieli Wykonawcy)

¹ Zgodnie z art. 4 pkt. 14 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634) przez grupę kapitałową rozumie się wszystkich przedsiębiorców, który są kontrolowani w sposób bezpośredni lub pośredni przez jednego przedsiębiorcę, w tym również tego przedsiębiorcę.