CIOP PIB

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy

nr sprawy: TA/ZO-37/2020

Zapytanie ofertowe dla zamówienia, do którego nie mają zastosowania przepisy ustawy Pzp

Przedmiot zamówienia: Przedłużenie wsparcia i aktualizacji (roczny abonament na odnowienie subskrypcji) do posiadanych przez Instytut 467 szt. licencji na oprogramowanie antywirusowe.

Rozdział 1 - Nazwa i adres Zamawiającego

Korespondencja pisemna: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, ul. Czerniakowska 16, 00-701 Warszawa;

Czynne w dni robocze w godz. 8^{00} - 16^{00}.

Osoby uprawnione do kontaktów z Wykonawcami: Urszula Wysocka;

E-mail/telefon do korespondencji: urwys@ciop.pl, tel. 22 623 46 30

Rozdział 2 - Tryb udzielenia zamówienia

Postępowanie prowadzone jest w trybie zapytania ofertowego, zwanego dalej ZO, do którego nie mają zastosowania przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843), zwanej dalej „ustawą Pzp".

Rozdział 3 - Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa przedłużenia wsparcia i aktualizacji (roczny abonament na odnowienie subskrypcji) do posiadanych przez Instytut 467 szt. licencji na oprogramowanie antywirusowe BROADCOM Symantec Endpoint Protection, ACD-GOV- na 12 miesięcy (od 28.11.2020 do 28.11.2021) - lub dostawa rozwiązania antywirusowego równoważnego tj. licencji na oprogramowanie równoważne, łącznie z instalacją i skonfigurowaniem oprogramowania równoważnego na 467 komputerach Zamawiającego w siedzibach w Warszawie (ul. Czerniakowska 16) i w Łodzi (ul. Wierzbowa 48) oraz przeszkoleniem użytkowników oraz administratorów w zakresie jego użytkowania w obu siedzibach. Warunki równoważności na oprogramowanie antywirusowe równoważne zawiera Szczegółowy opis przedmiotu zamówienia, przedstawiony poniżej.

Instytut w roku 2020 posiada następujące aktywne licencje na ww. oprogramowanie antywirusowe BROADCOM Symantec:

Nazwa	Ilość szt.
Endpoint Protection, License, ACD-GOV 50-99 Devices Qty: Start Date: 28-NOV-2019 End Date: 28-NOV-2020 (od 28.11.2019 do 28.11.2020) NR: M1338836489	57
Endpoint Protection, License, ACD-GOV 250-499 Qty: Start Date: 28-NOV-2019 End Date: 28-NOV-2020 (od 28.11.2019 do 28.11.2020) NR: M8538536264	377
Endpoint Protection, License, ACD-GOV 1-24 Devices Qty: Start Date: 28-NOV-2019 End Date: 28-NOV-2020 (od 28.11.2019 do 28.11.2020) NR: M9930384712	20
Endpoint Protection, License, ACD-GOV 1-24 Devices Qty: Start Date: 28-NOV-2019 End Date: 28-NOV-2020 (od 28.11.2019 do 28.11.2020) NR: S8570039546	9

Endpoint Protection, License, ACD-GOV 1-24 Devices Qty: Start Date: 28-NOV-2019 End Date: 28-NOV-2020 (od 28.11.2019 do 28.11.2020) NR: M6569881186	4

Szczegółowy opis przedmiotu zamówienia stanowi Załącznik nr 1 do Zapytania Ofertowego.

Jeżeli użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty lub pochodzenie, Zamawiający dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w opisie przedmiotu zamówienia, kompatybilne z posiadaną przez Zamawiającego infrastrukturą sieciowo-systemowo-sprzętową w tym samym zakresie, co produkty określone w opisie przedmiotu zamówienia. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. W przypadku złożenia oferty równoważnej (dotyczy również sprzętu o lepszych parametrach), składający ofertę ma obowiązek wykazania zgodności produktów poprzez porównanie parametrów oferowanych produktów z parametrami przedmiotu zamówienia.

Nazwa i kod według Wspólnego Słownika Zamówień (CPV):

48000000-8 – Pakiety oprogramowania i systemy informatyczne
72263000-6 – Usługi wdrażania oprogramowania
72611000-6 – Usługi w zakresie wsparcia technicznego

Rozdział 4 - Termin wykonania zamówienia

Termin realizacji przedmiotu zamówienia: **do 14 dni od dnia podpisania umowy.**

Rozdział 5 - Informacje dotyczące ofert częściowych i wariantowych

Zamawiający nie dopuszcza możliwości składania ofert częściowych i wariantowych.

Rozdział 6 - Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny ich spełniania, w tym wymagane dokumenty potwierdzające spełnianie warunków (o ile są wymagane)

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu:

a) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów;

   Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku.

b) sytuacji ekonomicznej lub finansowej umożliwiającej realizację przedmiotu zamówienia;

   Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku.

c) zdolności technicznej lub zawodowej w zakresie realizacji przedmiotu zamówienia:

Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku.

Rozdział 7 – Informacja o sposobie porozumiewania się

1. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami jest **Urszula Wysocka,** adres: urwys@ciop.pl ;
2. We wszelkiej korespondencji kierowanej do Zamawiającego drogą elektroniczną dotyczącej niniejszego postępowania należy wskazywać numer sprawy oraz nazwę postępowania.

Rozdział 8 – Termin związania ofertą

Wykonawca będzie związany ofertą przez okres **30 dni**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział 9 – Opis sposobu przygotowania oferty

1. Wykonawca zobowiązany jest przygotować ofertę zgodnie z wymaganiami określonymi w ZO.
2. Treść oferty musi odpowiadać treści niniejszego zapytania ofertowego.
3. Wykonawca może złożyć tylko jedną ofertę.
4. Ofertę należy przygotować w języku polskim.
5. Oferta powinna być podpisana przez osoby upoważnione do jej podpisania zgodnie z zasadami reprezentacji z aktualnego wpisu do właściwych rejestrów/ewidencji lub przez pełnomocnika/pełnomocników zgodnie z zakresem załączonego pisemnego pełnomocnictwa. Jeśli upoważnienie nie wynika z ogólnie dostępnych danych rejestrowych (wpis KRS, CEIDG) wówczas należy załączyć dokument poświadczający umocowanie danej osoby/ osób do podpisania oferty.
6. Wszelkie poprawki w tekście oferty muszą być naniesione w czytelny sposób i parafowane przez upoważnioną(e) osobę(y).
7. **Zamawiający wymaga, aby oferta zawierała co najmniej:**

1)	Formularz ofertowy – Załącznik nr 2 do ZO
2)	Oświadczenie o braku powiązań kapitałowych i osobowych – Załącznik nr 3 do ZO
3)	Pełnomocnictwo – jeśli dotyczy

Rozdział 10 – Miejsce oraz termin składania ofert

1. Ofertę należy złożyć do dnia: **25.11.2020 r. godz. 11^00** (decyduje data i godzina wpływu do CIOP-PIB).
2. Dopuszcza się złożenie oferty:

a) w formie pisemnej w siedzibie Zamawiającego: **CIOP-PIB, ul. Czerniakowska 16, 00-701 Warszawa – pok. 6 (parter) – Kancelaria;**
b) lub za pośrednictwem poczty elektronicznej (jako skan podpisanej oferty i załączników) na adres: **urwys@ciop.pl**

3. W tytule wiadomości/na kopercie proszę podać numer zapytania tj: **„Zapytanie ofertowe nr TA/ZO-37/2020".**
4. **Oferty otrzymane przez Zamawiającego po terminie składania ofert zostaną pozostawione bez rozpatrzenia.**

Rozdział 11 – Opis sposobu obliczenia ceny

1. Wykonawca uwzględniając wszystkie wymogi, o których mowa w niniejszym ZO, powinien w cenie brutto za realizację przedmiotu zamówienia ująć wszelkie koszty niezbędne dla prawidłowego wykonania przedmiotu zamówienia oraz uwzględnić inne opłaty i podatki, a także ewentualne upusty i rabaty.
2. Cena podana w ofercie nie podlega zmianom przez cały okres obowiązywania umowy.
3. Cenę należy wyrazić w PLN, z dokładnością do dwóch miejsc po przecinku.
4. Wszelkie rozliczenia, pomiędzy Zamawiającym a Wykonawcą, będą prowadzone w PLN.

Rozdział 12 – Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Oceniane kryteria i ich waga

KRYTERIUM	waga	SPOSÓB OBLICZANIA
Oferowana cena [wartość brutto]	100%	**Wartość punktowa = 100*Cmin/Cn** c_{min} - cena najniższa spośród złożonych ofert c_n - cena oferty badanej

2. Obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.
3. Oferta, która uzyska najwyższą ilość punktów w ww. kryterium oceny ofert zostanie uznana za najkorzystniejszą, pozostałe oferty zostaną sklasyfikowane zgodnie z ilością uzyskanych punktów.
4. Jeżeli nie będzie można wybrać oferty najkorzystniejszej z uwagi na to, że zostaną złożone oferty o takiej samej cenie, zamawiający wezwie wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych.
5. Wykonawcy składając oferty dodatkowe nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

Rozdział 13 – Informacje o wykluczeniu

1. Z udziału w postępowaniu wyłączone są osoby, które powiązane są z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się

wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:

a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;

b) posiadaniu co najmniej 10 % udziałów lub akcji;

c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;

d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.

2. W celu wskazania braku podstaw do wykluczenia Wykonawcy obowiązani są przedłożyć Oświadczenie, którego wzór stanowi Załącznik nr 2 do ZO.

3. Wykonawcy, którzy nie przedłożą oświadczenia o braku podstaw do wykluczenia, zostaną odrzuceni z przyczyn formalnych.

Rozdział 14 – Odrzucenie oferty

1. W niniejszym postępowaniu zostanie odrzucona oferta Wykonawcy który:

a) złoży ofertę niezgodną z treścią niniejszego zapytania ofertowego,

b) przedstawi nieprawdziwe informacje,

c) nie spełnia warunków udziału w postępowaniu,

d) złożył ofertę po terminie składania ofert;

e) podlega wykluczeniu z udziału w postępowaniu o udzielenie zamówienia.

Rozdział 15 – Informacje dotyczące RODO

1. Klauzula informacyjna z art. 13 RODO związana z niniejszym postępowaniem o udzielenie zamówienia publicznego

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1) Administratorem Pani/Pana danych osobowych jest Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy z siedzibą przy ul. Czerniakowska 16, 00-701 Warszawa;
2) Administrator danych osobowych powołał Inspektora Ochrony danych nadzorującego prawidłowość przetwarzania danych osobowych, z którym można skontaktować się za pośrednictwem adresu e-mail: iod@ciop.pl;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego nr **TA/ZO-37/2020** na; **„Przedłużenie wsparcia i aktualizacji (roczny abonament na odnowienie subskrypcji) do posiadanych przez Instytut 467 szt. licencji na oprogramowanie antywirusowe.".**

4) 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;
5) W przypadku danych osobowych zamieszczonych przez Zamawiającego w Biuletynie Zamówień Publicznych, Prezes UZP zapewnia techniczne utrzymanie systemu oraz określa okres przechowywania danych osobowych w BZP.
6) Zasada jawności ma zastosowanie do wszystkich danych osobowych, z wyjątkiem danych, o których mowa w art. 9 RODO.
7) W odniesieniu do danych osobowych w kategorii dane wrażliwe dotyczące wyroków skazujących, o których mowa w art. 10 RODO Zamawiający będzie udostępniał te dane jedynie w sytuacji, w której ujawnianie jest niezbędne w celu umożliwienia korzystania ze środków ochrony prawnej do upływu terminu do ich wniesienia.
8) 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;
9) 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;
10) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
11) posiada Pani/Pan:
    a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
    (Jeżeli wykonanie tego obowiązku wymagać będzie niewspółmiernie dużego wysiłku, Zamawiający może żądać, od osoby, której dane dotyczą wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego).
    b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *(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);*
    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 (*prawo do ograniczenia przetwarzania nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielnie zamówienia publicznego. Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 RODO, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, zamawiający nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 RODO).*
    c) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
12) nie przysługuje Pani/Panu:
    a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
    b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
    c) 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.

13) W przypadku udostępnienia do CIOP-PIB przez Podmiot biorący udział w niniejszym postępowaniu o udzielenie Zamówienia, będący adresatem niniejszego dokumentu, danych osobowych swoich pracowników, pełnomocników, członków zarządu, wspólników, współpracowników, kontrahentów, dostawców, beneficjentów rzeczywistych lub innych osób, CIOP-PIB wnosi o poinformowanie tych osób:
   a) zakresie danych osobowych dotyczących tych osób, a przekazanych CIOP-PIB,
   b) tym, że CIOP-PIB jest administratorem ich danych osobowych oraz że przetwarza ich dane osobowe na zasadach określonych powyżej,
   c) tym, że ww. Podmiot jest źródłem, od którego CIOP-PIB pozyskała ich dane.

Rozdział 16 – Udzielenie zamówienia

1. Zamawiający zastrzega możliwość unieważnienia postępowania bez podania przyczyny.
2. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą po dokonaniu oceny ofert zgodnie z zasadami opisanymi w rozdziale 12.
3. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza będzie poinformowany o terminie przeprowadzenia negocjacji lub podpisania umowy.
4. Wybrany Wykonawca ma obowiązek zawrzeć umowę, której warunki określono we Wzorze umowy, stanowiącym Załącznik nr 4 do ZO.
5. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie umowy z kolejnym Wykonawcą, który w postępowaniu o udzielenie zamówienia uzyskał kolejną najwyższą liczbę punktów.
6. Umowę może podpisać w imieniu Wykonawcy osoba (osoby) upoważniona(e) do reprezentowania Wykonawcy.

Rozdział 17 - Załączniki

Nr Załącznika	Nazwa Załącznika
1	Szczegółowy opis przedmiotu zamówienia
2	Formularz oferty
3	Oświadczenie o braku powiązań osobowych i kapitałowych
4	Wzór umowy

Załącznik nr 1 do ZO

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa przedłużenia wsparcia i aktualizacji (rocznego abonamentu na odnowienie subskrypcji) do posiadanych i eksploatowanych przez Zamawiającego 467 szt. Licencji akademickich (ACD-GOV) na oprogramowanie antywirusowe lub dostawa rozwiązania antywirusowego równoważnego.

Zamawiający posiada obecnie i eksploatuje licencje na oprogramowanie **antywirusowe BROADCOM Symantec Endpoint Protection** w wersji 14.3 (467 licencji akademickich) z wykupioną pomocą techniczną i aktualizacją do 27.11.2020 r.

W związku z wykonaną instalacją, konfiguracją i pomyślną eksploatacją ww. oprogramowania antywirusowego na przestrzeni kilku lat do chwili obecnej na zestawie 467 indywidualnie użytkowanych komputerach (z systemami operacyjnymi MS Windows 7, 8.x, 10 32 lub 64-bit), Zamawiający oczekuje w ramach przedmiotu zamówienia dostawy **przedłużenia wsparcia i aktualizacji (rocznego abonamentu na odnowienie subskrypcji) do posiadanych przez Instytut 467 szt. Licencji akademickich** (ACD-GOV) **na ww. oprogramowanie antywirusowe na kolejne 12 miesięcy użytkowania t.j. od dnia 28.11.2020 do dnia 27.11.2021 r.** lub dostawy rozwiązania antywirusowego równoważnego.

WARUNKI RÓWNOWAŻNOŚCI

Dostawa **rozwiązania antywirusowego równoważnego** obejmuje doprowadzenie ww. zestawu komputerów indywidualnych Zamawiającego z systemami operacyjnymi MS Windows 7, 8.x, 10, 32 lub 64-bit do stanu co najmniej równego obecnemu pod względem lokalnej ochrony antywirusowej, tj.:

1. Dostawę 467 szt. Licencji wieczystych na oprogramowanie antywirusowe równoważne o parametrach co najmniej takich, jak wymienione w tabeli nr 2, z 12-miesięcznym abonamentem na wsparcie techniczne i aktualizację baz zagrożeń
2. Odinstalowanie dotychczas użytkowanego oprogramowania antywirusowego (przez Wykonawcę) oraz wykonanie (przez Wykonawcę) instalacji i skonfigurowania ww. oprogramowania równoważnego na 467 komputerach Zamawiającego w siedzibach Zamawiającego w Warszawie i w Łodzi
3. Przeszkolenie wszystkich użytkowników ww. komputerów oraz dwóch administratorów w zakresie funkcjonalności, własności interfejsu oraz użytkowania ww. oprogramowania antywirusowego równoważnego oraz jego systemu zarządzania
4. 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.

5. Wraz z produktem równoważnym Wykonawca jest zobowiązany do dostarczenia następujących dokumentów:
   a. pełnego postanowienia licencji / sublicencji produktu równoważnego,
   b. pełnego wykazu funkcjonalności produktu równoważnego, co najmniej zgodnego z wymaganiami minimalnymi określonymi w Tabeli 2
   c. pełnych warunków i zasad świadczenia usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji dla produktu równoważnego,
   d. wykazu miejsc zastosowania produktu równoważnego.

Tabeli 2. **Minimalna charakterystyka wymagana**

		Oprogramowanie antywirusowe do lokalnego zastosowania na komputerach indywidualnych - najnowsza wersja, wersja polska, wersja edukacyjna (akademicka) - 467 szt. Licencji wieczystych + nośnik 1 szt.	**TYP oferowany: .....** **Producent: .....**
	Funkcja / parametr	**Minimalna charakterystyka wymagana**	**Parametry oferowane nie gorsze, niż wymagane** (w polach, w których jest to wymagane, wpisać **wartość**, w pozostałych **wpisać „Tak" lub „Nie")**
	Potwierdzenie skuteczności ochrony	Zamawiający dopuszcza oprogramowanie antywirusowe, którego skuteczność ochrony potwierdzona jest przez renomowane organizacje publiczne zajmujące się bezpieczeństwem komputerowym w niezależnych testach oprogramowania, których aktualne wyniki opublikowano na stronie: https://www.av-test.org/en/antivirus/business-windows-client/	
	Poziom wykrywalności zagrożeń	Ogólna wykrywalność różnego typu zagrożeń (*Protection*) nie może być mniejsza niż na poziomie ocenionym na 6 pkt, potwierdzona w testach (ochrona w czasie rzeczywistym), których wyniki opublikowano na stronie (https://www.av-test.org/en/antivirus/business-windows-client/)	
	Poziom wpływu	Poziom wpływu na spowolnienie pracy systemu	

	na spowolnienie pracy systemu komputerowego (pracującego pod systemem Windows 7,8/8.1,10)	komputerowego (*Performance*) nie może być oceniony na mniej niż 6 pkt. wg testów, których wyniki opublikowano na stronie (https://www.av-test.org/en/antivirus/business-windows-client/)	
	Funkcjonalność i jakość interfejsu użytkownika	Poziom funkcjonalności i jakości interfejsu użytkownika (*Usability*) nie może być oceniony na mniej niż 6 pkt. wg testów, których wyniki opublikowano na stronie (https://www.av-test.org/en/antivirus/business-windows-client/)	
	Wsparcie techniczne i zasady aktualizacji	• min. 1 rok od daty zakupu • kompletne aktualizacje produktu/pakietu w tym okresie • możliwość przedłużenia subskrypcji na kolejny okres wraz z aktualizacją oprogramowania do najnowszej dostępnej wersji	**Oferowany okres wsparcia technicznego i aktualizacji:** .....
	Zgodność z aktualnym oprogra-mowaniem Zamawiającego	Zgodność oprogramowania typu Klient z oprogramowaniem Symantec Endpoint Protection Manager z pakietu Symantec Endpoint Protection (wykorzystywanym obecnie w liczbie **492** licencji przez Zamawiającego)	
	Zgodność z systemem operacyjnym	Wymagana pełna zgodność z systemami: 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.	
		Wymagane komponenty oprogramowania takie jak: firewall, zapobieganie włamaniom (IPS), 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.	
	Wymagane funkcje/ parametry	**Wymagania funkcjonalne dla równoważnego oprogramowania antywirusowego (produktu)**	
	Ochrona antywirusowa:	Usuwanie wirusów, makro-wirusów, robaków internetowych oraz koni trojańskich (oraz	

		wirusów i robaków z plików skompresowanych oraz samo rozpakowujących 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 musi 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:	
		• na dyskach twardych	
		• w boot sektorach	
		• na dyskietkach	
		• na płytach CD/DVD	
		• na zewnętrznych nośnikach pamięci (np. podłączonych przez port USB).	
		Wymagana możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej.	
		Wymagana możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.	
		Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek.	
		Wymagana funkcjonalność wyszukiwania/usuwania 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.	
		Wymagana możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących - powrót do poprzedniego zastawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów.	
		Wymagana możliwość natychmiastowego "wypchnięcia" definicji wirusów do stacji klienckich	
		Wymagana aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej trzy razy dziennie.	
		Wymagana 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 nie autoryzowanych prób zmian rejestru dokonywanych przez użytkownika.	
		Automatyczne ponowne uruchomianie 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 ilość 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 aplikacje, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 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.	
		Wymagana możliwość wyboru wielkości definicji antywirusowych, z której będzie korzystał zainstalowany agent - system musi posiadać pełna wersję sygnatur oraz ich wersję uproszczoną znacząco mniejszą o pełnej do instalacji na systemach z niewielką ilością miejsca na dyskach oraz w systemach VDI.	
		Możliwość konfiguracji oraz personalizacji ustawień oprogramowania	
		Małe zapotrzebowanie na zasoby pamięci operacyjnej i systemu	
		System centralnego zarządzania aktualizacjami	
		Ustawienia alternatywnego źródła pobierania	

		baz sygnatur wirusów	
		Automatyczna aktualizacja silnika skanującego oraz bazy sygnatur wirusów	
		Automatyczne skanowanie w tle	
		Automatyczne skanowanie i monitorowanie operacji związanych z uruchamianiem programów, plików oraz operacji zapisu danych na HDD i nośnikach przenośnych	
		Automatyczne, bezobsługowe wykrywanie, analiza i usuwanie makrowirusów	
		Automatyczne leczenie zainfekowanych plików bądź blokada dostępu do pliku	
		Automatyczne przenoszenie zablokowanego pliku do systemu kwarantanny	
		Skanowanie na żądanie: • dysku • plików • folderów	
		Skanowanie: • w czasie rzeczywistym • ruchu internetowego POP3 i http • poczty wychodzącej/przychodzącej • uruchamianych procesów i plików z nimi powiązanych • wszystkich plików na HDD w tym plików systemowych i ukrytych • pamięci operacyjnej, • rekordów rozruchowych dysków • archiwów ZIP, RAR, ARJ, LZH/LHA, MIME/UU, CAB, PKLite, LZEXE • dokumentów pakietu MS Office • danych NTFS	
		Heurystyczne wykrywanie nowych nie sklasyfikowanych wirusów	
		Blokowanie niebezpiecznych skryptów	
		Dzienniki zdarzeń: • zdarzeń • Infekcji • skanera na żądanie	
		Harmonogram zadań • skanowań • aktualizacji	

	System Firewall:	Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.	
		Moduł firewall musi mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.	
		Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać.	
		Program musi 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 musi się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji.	
		Konfiguracja stacji musi się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji DNS (FQDN) lub domeny DNS.	
		Firewall musi mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach, musi istnieć możliwość dodania własnego komunikatu.	
		W przypadku wykrycia zdefiniowanego ruchu, firewall musi wysłać wiadomość do administratora.	
		Wymagane uniemożliwianie określenia systemu operacyjnego, rodzaju przeglądarki internetowej przez serwery www.	
		Wymagane uniemożliwianie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację.	
		Wymagane uniemożliwianie przejęcia sesji poprzez losowo generowane numery sekwencji TCP	
		Wymagane domyślne reguły zezwalające na ruch DHCP, DNS, WINS.	
	System IPS -	Producent musi dostarczyć bibliotekę ataków i	

	ochrona przed włamaniami	podatności (sygnatur) stosowanych przez produkt.	
		Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.	
		Produkt musi 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. Musi 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 musi umożliwiać uruchamianie i blokowanie wskazanych aplikacji.	
		Produkt musi umożliwiać ładowanie modułów lub bibliotek DLL.	
		Produkt musi umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje.	
		Aplikacje muszą być rozróżniane poprzez nazwę i sygnaturę cyfrową.	
		Produkt musi umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika.	
		Produkt musi kontrolować dostęp do rejestru	

		systemowego.	
		Produkt musi umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne.	
		Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych.	
		Polityki ochrony muszą mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu.	
		Wymagana możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego.	
		Wymagana możliwość utworzenie 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.	
		Wymagana możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, by tylko aplikacje znajdujące się na liście nie mogły uruchomić się na komputerze.	
		Wymagana możliwość automatycznego importu list zarówno białej, jaki 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 muszą być przeprowadzane cyklicznie, co zdefiniowany okres czasu.	
		Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta.	
		Oprogramowanie musi umożliwiać wykonanie nie standardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać	

		zaawansowaną składnie If ... Then ... Else.	
		W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:	
		○ Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne	
		○ Pliki - istnienie, data, rozmiar, suma kontrolna	
		○ Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego	
		○ Zainstalowane poprawki	
		○ Uruchomiony proces, wersja systemu operacyjnego	
		○ Własna aplikacja	
		W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako dostępne operacje do wykonania, musi istnieć możliwość:	
		○ Uruchamianie dowolnego/własnego skryptu lub programu	
		○ Logowanie zdarzenia	
		○ Ukazanie okienka z wiadomością	
		○ Pobieranie oraz uruchamianie instalacji	
		○ Musi istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.	
		Musi istnieć 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.	
	Ochrona	Produkt musi umożliwiać identyfikacje	

	środowisk wirtualnych:	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. VOl, w szczególności tzw. "non-persistent".	
		Produkt musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń.	
	Moduł raportujący:	Produkt musi zapewniać graficzne raportowanie.	
		Wbudowane raporty muszą pokazywać co najmniej:	
		○ stan dystrybucji sygnatur antywirusowych, sygnatur heurystycznych oraz IDS/IPS	
		○ wersje zainstalowanych klientów	
		○ inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor)	
		○ wykryte wirusy, zdarzenia sieciowe, integralności komputerów	
		○ zainstalowane technologie i ich aktualny stan	
		Moduł raportowania musi pokazywać stan wykonywanych poleceń na komputerach.	
		Wymagana 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 postacie kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwijanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór intersujących 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 musi wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Musi istnieć możliwość blokowania takich zmian.	
		Produkt musi zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli musi być możliwy po wcześniejszej weryfikacji użytkownika. Produkt musi mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.	
		Wymagana 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 muszą być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.	
		Uprawnienia administratorów muszą być ustawiane niezależnie dla każdego	
		kontenera wewnątrz organizacji.	
		Wymagana możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.	
		Konfiguracja agentów musi mieć strukturę drzewa, z mechanizmami dziedziczenia.	
		Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika musi być konfigurowany z poziomu centralnej konsoli zarządzającej.	

		Konfiguracja aktywna na stacji musi rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.	
		Lokalizacja musi 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 musi zawierać możliwość tworzenia połączeń logicznych "I" oraz "LUB" na powyżej wymienionych elementach.	
		Paczki instalacyjne produktu muszą 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 muszą być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.	
		Produkt musi automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.	
		Wymagana możliwość zdefiniowania alertów administracyjnych zawierających co najmniej zdarzenia:	
		• błędnej autoryzacji do systemu zarządzania	
		• dostępności nowego oprogramowania	
		• pojawienia się nowego komputera	
		• zdarzeń powiązanych z infekcjami wirusów	
		• stanu serwerów zarządzających	
		Wymagana możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji.	
		Wymagana oficjalna dokumentacja schematu bazy danych, z której korzysta system	

		zarządzający.	
		Wymagana **pełna polska wersja językowa** oprogramowania dla **systemu zarządzania i stacji klienckich** wraz z dokumentacją.	

Załącznik nr 2 do ZO

Formularz oferty

Postępowanie nr TA/ZO-37/2020

I. DANE WYKONAWCY:	
Nazwa Wykonawcy:	
Adres lub siedziba:	
Numer KRS (jeśli dotyczy)	
Numer NIP (jeśli dotyczy):	
Osoba upoważniona do kontaktu z Zamawiającym	1) Imię i nazwisko: ..... 2) tel.: ..... 3) adres e-mail: .....
Nr konta bankowego, na które będzie kierowane wynagrodzenie dla Wykonawcy, w przypadku podpisania umowy	..... **Wykonawca zobowiązany jest do podania numeru rachunku bankowego, który widnieje w Wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, prowadzonym przez Ministerstwo Finansów**

II. CENA OFERTY:		
Wartość netto	..... zł	słownie: .....
Wartość podatku VAT	(.....% VAT).....zł	słownie: .....
Wartość brutto	..... zł	słownie: .....

III. NAZWA OPROGRAMOWANIA:

Oferuje licencję:

1. ..... w ilości szt. .....
2. ..... w ilości szt. .....
3. ..... w ilości szt. .....
4. ..... w ilości szt. .....
5. ..... w ilości szt. .....

OŚWIADCZAMY, ŻE:

1) w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia i realizacji przyszłego świadczenia umownego;
2) zapoznaliśmy się z ZO, akceptujemy je w całości i nie wnosimy do niego zastrzeżeń;
3) zapoznaliśmy się z postanowieniami wzoru umowy i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na określonych warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego;
4) jesteśmy związani niniejszą ofertą przez okres **30 dni** od dnia upływu terminu składania ofert.
5) w przypadku wyboru naszej oferty, wskazujemy następujące osoby do umieszczenia w umowie, jako reprezentacja Wykonawcy, zgodnie z wpisem w CEiDG / Krajowym Rejestrze Sądowym /udzielonym pełnomocnictwem*:
   - ✓ Imię i nazwisko - .....
   - ✓ stanowisko/funkcja .....
6) Wraz z ofertą składamy następujące oświadczenia i dokumenty:

   .....

   .....
7) wypełniliśmy 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[1].

Zaznaczyć właściwe

I. PODPIS I PIECZĘĆ WYKONAWCY

..... *(miejscowość i data)*	..... *(Podpis Wykonawcy/ Pełnomocnika)*

[1] W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Załącznik nr 3 do ZO

....., dn. .....

Oświadczenie o braku powiązań osobowych lub kapitałowych
Znak sprawy: TA/ZO-37/2020

Ja, niżej podpisany(a)

.....

reprezentujący
firmę.....

oświadczamy, że **nie jestem** powiązany osobowo lub kapitałowo z Zamawiającym. Przez powiązania osobowe lub kapitałowe rozumie się wzajemne powiązania lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy, polegające w szczególności na:

a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
b) posiadaniu najmniej 10% udziałów lub akcji;
c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.

.....
(podpis upoważnionego przedstawiciela Wykonawcy i ew. pieczątka)

Załącznik nr 4 do ZO

Wzór umowy

zawarta w dniu ..... roku w Warszawie w wyniku postępowania przeprowadzonego w trybie zapytania ofertowego, pomiędzy:

ZAMAWIAJĄCYM: Centralnym Instytutem Ochrony Pracy - Państwowym Instytutem Badawczym, adres siedziby: 00-701 Warszawa, ul. Czerniakowska 16, instytutem badawczym posiadającym status państwowego instytutu badawczego, wpisanym do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod Nr KRS: 0000033480, posiadającym NIP: 525-000-82-70, reprezentowanym przez:

.....

.....

a

WYKONAWCĄ: .....

(1) .....
*(**w przypadku podmiotów wpisanych do KRS** należy podać pełną nazwę (firmę) zgodnie z wpisem do rejestru, oraz dokładny adres siedziby)*, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy .....

..... Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: ..... , NIP ....., REGON ....., kapitał zakładowy w wysokości ..... zł *(**dotyczy tylko spółek kapitałowych**)*, kapitał opłacony ..... *(**dotyczy tylko spółek akcyjnych**)*, zwaną/zwanym dalej „**Wykonawcą**", reprezentowaną/reprezentowanym zgodnie z zasadami reprezentacji wskazanymi w ww. rejestrze przez:

.....

(2).....
*(**w przypadku osób fizycznych wpisanych do CEIDG** należy podać imię i nazwisko, adres zamieszkania, NIP, REGON, adres głównego miejsca prowadzenia działalności gospodarczej,, adres do doręczeń)*

.....
przedsiębiorcą wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod nazwą (firmą): .....
.....

działającym osobiście / reprezentowanym przez .....

.....
(3) ***w przypadku spółki cywilnej*** *należy podać Imiona i nazwiska wspólników. ich NIP-y, nazwę (firmę spółki), NIP i REGON tej spółki oraz adres do doręczeń)* zwanymi dalej **Wykonawcą,** reprezentowanymi zgodnie z zasadami reprezentacji zawartymi w uwierzytelnionym przez jego wystawców dokumencie pt. ..... stanowiącym załącznik nr..... **, zgodnie z załączonym pełnomocnictwem** / pełnomocnictwami** stanowiących/mi załącznik Nr ..... do umowy **, przez:

.....

o następującej treści:

§ 1

1. Przedmiotem niniejszej umowy jest **roczny abonament na odnowienie subskrypcji oprogramowania antywirusowego ..... na 467 komputery wraz z dokumentem licencyjnym** zwane dalej przedmiotem umowy. Opis Przedmiotu umowy stanowi Załącznik nr 1 do niniejszej umowy – Formularz cenowy z ..... r.
2. Wykonawca zobowiązuje się zrealizować Przedmiot umowy w terminie do ....2020 r.
3. Wykonawca oświadcza i zapewnia, że jest uprawniony do dystrybucji subskrypcji oprogramowania będącego przedmiotem umowy.
4. Wykonawca zobowiązany jest do niezwłocznego informowania Zamawiającego o zdarzeniach mających lub mogących mieć wpływ na wykonanie umowy, w tym o wszczęciu wobec niego postępowania egzekucyjnego, naprawczego, upadłościowego (układowego lub likwidacyjnego).

§ 2

1. Odbiór Przedmiotu umowy przeprowadzi Komisja Zamawiającego. Z przeprowadzonego odbioru Komisja sporządzi Protokół Odbioru.
2. Protokół Odbioru musi zawierać w szczególności:
   1) opis Przedmiotu umowy: firmę producenta, nazwy i rodzaje oraz inne występujące oznakowania;
   2) potwierdzenie aktywności dostępu do aktualizacji oprogramowania, wskazanego w § 1 ust.1 i okresu tej aktualizacji;
   3) miejsce i datę odbioru;
   4) datę i miejsce sporządzenia protokołu oraz podpisy członków Komisji.

§ 3

1. Za wykonanie Przedmiotu umowy potwierdzone Protokołem odbioru podpisanym przez Komisję Zamawiającego bez żadnych zastrzeżeń, Wykonawca otrzyma wynagrodzenie w kwocie ..... zł netto (.....), plus podatek VAT w wysokości 23 % tj. ..... zł, co łącznie stanowi kwotę: ..... zł brutto (..... płatne w terminie do 14 dni od daty otrzymania faktury wystawionej zgodnie z obowiązującymi przepisami prawa na rachunek bankowy Wykonawcy podany w doręczonej Zamawiającemu fakturze.
2. Za datę zapłaty Strony uznają dzień obciążenia rachunku Zamawiającego.
3. Wystawiona faktura ma być zgodna z przepisami ustawy o podatku od towarów i usług, w szczególności z art. 106e ust.1 pkt. 18e art. 108e ust.1e oraz art. 108e tej ustawy.
4. Wykonawca oświadcza, że rachunek bankowy wskazany w umowie/fakturze jest rachunkiem znajdującym się w elektronicznym wykazie podmiotów prowadzonym od 1 września 2019 r. przez Szefa Krajowej Administracji Skarbowej, o którym mowa w ustawie o podatku od towarów i usług.
5. W przypadku gdy rachunek bankowy Wykonawcy nie spełnia warunków określonych w pkt. 4 powyżej, opóźnienie w dokonaniu płatności w terminie określonym w umowie/fakturze powstałe w skutek braku możliwości realizacji przez Zamawiającego

płatności wynagrodzenia na rachunek objęty Wykazem, nie stanowi dla Wykonawcy podstawy do żądania od Zamawiającego jakichkolwiek odsetek, jak również innych rekompensat/odszkodowań/roszczeń z tytułu dokonania nieterminowej płatności.

§ 4

1. W przypadku nie wykonania przez Wykonawcę umowy Zamawiający ma prawo odstąpić od umowy w terminie 14 dni od dnia wskazanego w § 1 ust.2. a Wykonawca na żądanie Zamawiającego zapłaci karę umowną z tytułu odstąpienia przez Zamawiającego od umowy w wysokości 30 % wynagrodzenia brutto określonego w § 3 ust. 1,
2. W przypadku zwłoki w wykonaniu Przedmiotu umowy Wykonawca na żądanie Zamawiającego zapłaci karę umowną w wysokości 0,5 % wynagrodzenia brutto określonego w § 3 ust. 1, za każdy dzień zwłoki, licząc od terminu dostarczenia Przedmiotu umowy wskazanego w § 1 ust.2. a jeżeli zwłoka przekroczy 14 dni, Zamawiający może odstąpić od umowy w terminie 14 dni licząc od pierwszego dnia przekroczenia terminu.
3. Zamawiający ma prawo dochodzenia odszkodowania przekraczającego wysokość zastrzeżonych kar umownych, do wysokości rzeczywiście poniesionej straty na zasadach ogólnych.
4. Odpowiedzialność Stron z tytułu nienależytego wykonania lub niewykonania umowy wyłączają jedynie zdarzenia siły wyższej. Zdarzeniami siły wyższej są zdarzenia zewnętrzne, nagłe, niezależne od woli Stron, których nie można było przewidzieć i którym nie można było zapobiec, a które mają wpływ na wykonanie niniejszej umowy.
5. Jeśli w ciągu 14 dni od pisemnego powiadomienia drugiej Strony o zaistnieniu siły wyższej jej działanie nie ustanie, Strony spotkają się w celu podjęcia działań dla uniknięcia dalszego opóźnienia w realizacji umowy.

§ 5

1. Wykonawca oświadcza, że wykonanie jego obowiązków wynikających z umowy nie będzie naruszać żadnych praw osób trzecich za co ponosi pełną odpowiedzialność.

§ 6

1. Niniejsza umowa reguluje wzajemny stosunek stron i obowiązki w zakresie przetwarzania danych osobowych:
   1) każda ze stron działając jako administrator danych osobowych przetwarza udostępnione jej przez drugą stronę dane osobowe osób uczestniczących w zawarciu i wykonaniu przedmiotowej umowy wyłącznie w celu zawarcia i wykonania tej umowy,
   2) strony umowy oświadczają, że osobom występujących po ich stronie przy zawarciu| i wykonaniu przedmiotowej umowy znane są informacje, które powinny być im przekazane zgodnie z art. 13 ust.1-3 lub art.14 ust. 1-4 RODO a tym samym, zgodnie z art. 13 ust. 4 i art. 14 ust. 5 RODO każda ze stron nie ma obowiązku przekazania tym osobom tych informacji.
2. Zamawiający oświadcza, że na dzień zawarcia umowy posiada status dużego przedsiębiorcy w rozumieniu art. 4 pkt 6 ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (j.t. Dz. U. z 2020 r., poz. 935 z póź. zm.) zwanej dalej ustawą.
1. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy Kodeksu cywilnego, a także inne przepisy prawa powszechnie obowiązującego.
3. Ewentualne spory wynikłe z niniejszej umowy Strony będą starały się rozwiązać

w drodze porozumienia, jednak w razie braku możliwości osiągnięcia porozumienia spory rozstrzygać będzie sąd właściwy dla siedziby Zamawiającego.

4. Integralną część umowy stanowią:

- Załącznik nr 1 - opis Przedmiotu umowy tj. Formularz cenowy z dnia .....;
- Załącznik nr 2 – pełnomocnictwa przedstawicieli Zamawiającego;
- Załącznik nr 3 - wydruk z właściwego rejestru/ewidencji Wykonawcy.

3. Umowa niniejsza została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

ZAMAWIAJĄCY **WYKONAWCA**