Znak sprawy: KPB-V.273.29.2019

Specyfikacja Istotnych Warunków Zamówienia na zakup oprogramowania antywirusowego.

ZAMAWIAJĄCY

Łódzki Urząd Wojewódzki w Łodzi
ul. Piotrkowska 104
90 – 926 Łódź

ZATWIERDZAM

Mirosław Suski
Dyrektor Generalny Urzędu

Łódź, 11 września 2019 r.

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO.

Łódzki Urząd Wojewódzki w Łodzi
ul. Piotrkowska 104
90 – 926 Łódź
NIP: 725-102-84-65

Godziny pracy:
Poniedziałek, środa – piątek – 8.00. – 16.00.
Wtorek – 9.00. – 17.00.

II. TRYB UDZIELENIA ZAMÓWIENIA.

1. Zamówienie będzie udzielone w trybie **przetargu nieograniczonego,** zgodnie z art. 10 ust. 1 oraz art. 39 - 46 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2018 r., poz. 1986 ze zmianami), zwanej dalej „PZP".
2. Wartość zamówienia nie przekracza kwoty określonej w przepisach wydanych na podstawie art. 11 ust. 8 PZP.
3. Wykonawca powinien dokładnie zapoznać się z niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ" i złożyć ofertę zgodnie z jej wymaganiami.
4. Wszystkich Wykonawców uczestniczących w niniejszym postępowaniu obowiązuje działanie zgodnie z PZP wraz z przepisami wykonawczymi do PZP.
5. Załączniki do SIWZ stanowią jej integralną część.

III. OPIS PRZEDMIOTU ZAMÓWIENIA.

1. Przedmiotem zamówienia jest zakup i wdrożenie oprogramowania antywirusowego.
2. Szczegółowy opis przedmiotu zamówienia zawiera Załącznik Nr 1 do SIWZ.
3. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych we wzorze umowy stanowiącym Załącznik Nr 5 do SIWZ.
4. Nazwy i kody dotyczące przedmiotu zamówienia określone we Wspólnym Słowniku Zamówień Publicznych (CPV): 4876000-3 pakiety oprogramowania do ochrony antywirusowej

IV.TERMIN WYKONANIA ZAMÓWIENIA.

Wymagany termin wykonania zamówienia maksymalnie 14 dni od daty podpisania umowy (w tym terminie Zamawiający zleci do realizacji zamówienie, natomiast Wykonawca dostarczy zamówiony towar w terminie zaoferowanym przez siebie w formularzu oferty).

V. WARUNKI UDZIAŁU W POSTĘPOWANIU.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
   1) nie podlegają wykluczeniu;
   2) spełniają warunki udziału w postępowaniu.
      a) zdolności technicznej lub zawodowej:
      b) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów,
      c) sytuacji ekonomicznej i finansowej. Zamawiający nie określa szczegółowych warunków. Wykonawca spełni ww. warunki poprzez złożenie dokumentów, o których mowa w rozdz. VII ust. 1 SIWZ.

      - Zamawiający nie stawia szczegółowych warunków udziału w postępowaniu.
2. Zamawiający może, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.
3. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.

4. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
5. Z treści pełnomocnictwa będzie wynikał zakres umocowania.
6. Wszystkie dokumenty oferty wspólnej, z wyjątkiem oświadczenia Wykonawcy o spełnianiu warunków udziału w postępowaniu oraz o braku podstaw do wykluczenia – podpisuje pełnomocnik. Oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu oraz oświadczenie z art. 24 ust. 1 i ust. 5 pkt.1 PZP może być podpisane osobiście przez Wykonawcę lub w imieniu Wykonawcy przez pełnomocnika, jeżeli został on upoważniony do dokonania tej czynności.
7. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego każdy z Wykonawców wspólnie ubiegających się o zamówienie zobowiązany jest wykazać brak podstaw do wykluczenia go z postępowania na podstawie art. 24 ust. 1 i art. 24 ust. 5 pkt 1 PZP.
8. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, składa każdy z Wykonawców.
9. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia warunki, o których mowa w rozdz. V ust. 1 pkt 2 SIWZ zostaną spełnione wyłącznie jeżeli Wykonawcy ustanowią pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego;
4. Wykonawca może w celu potwierdzenia spełniania warunków w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
5. Wykonawca, który polega na zdolnościach technicznych lub zawodowych innych podmiotów udowodni Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów w stopniu umożliwiającym należyte wykonanie zamówienia publicznego w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
6. Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 12–22 i ust. 5 ust. 1 PZP.

VI. PODSTAWY WYKLUCZENIA, O KTÓRYCH MOWA W ART. 24 UST. 5. USTAWY.

Zamawiający przewiduje wykluczenie Wykonawcy w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2019 r. poz. 243 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2017 r. poz. 2344 ze zm.) zgodnie z art. 24 ust. 5 pkt 1 PZP.

VII. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAKU PODSTAW DO WYKLUCZENIA.

1. Do oferty każdy Wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenie w zakresie wskazanym w Załączniku nr 3 i 4 do SIWZ. Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie, o którym

mowa w ust. 1 składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to ma potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

3. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o podwykonawcach w oświadczeniu, o którym mowa w ust. 1.
4. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia - w zakresie, w jakim powołuje się na ich zasoby - warunków udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w ust. 1.
5. Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia dokumentów, o których mowa w ust. 6.
6. Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw do wykluczenia na podstawie o art. 24 ust. 5 pkt 1 PZP, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert – złożony w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem przez osobę uprawnioną do reprezentowania Wykonawcy.
7. Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 PZP, przekaże Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 PZP. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Wzór oświadczenia stanowi Załącznik Nr 6 do SIWZ.

   UWAGA! Oświadczenia nie należy dołączać do oferty.
8. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w ust. 6, składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Ww. dokumenty muszą być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
9. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w ust. 6, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby lub osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsca zamieszkania Wykonawcy lub miejsce zamieszkania tej osoby. Oświadczenie winno być złożone nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
10. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających spełnienie warunków udziału w postępowaniu i brak podstaw wykluczenia z postępowania, jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2017 roku, poz. 570 ze zm.).

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

1. Oferty oraz oświadczenia, o których mowa w art. 25a PZP Wykonawca składa, za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe, osobiście lub za pośrednictwem posłańca.
2. W pozostałym zakresie komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną lub faksem; nr faksu Zamawiającego (42) 664 – 11 – 05; adres poczty elektronicznej: zamowienia@lodz.uw.gov.pl
3. Dokumenty składane osobiście lub za pośrednictwem posłańca należy złożyć w siedzibie Zamawiającego sekretariat Biura Kadr, Płac i Budżetu, ul. Piotrkowska 104, 90 – 926 Łódź, bud. „E", I p., pok. 133, w godzinach pracy Zamawiającego.
4. Dokumentację uznaje się za złożoną w terminie, w którym dotarła do drugiej strony w sposób umożliwiający jej na zapoznanie się z jej treścią. W szczególności, w przypadku komunikowania się za pośrednictwem operatora pocztowego, o terminie złożenia dokumentacji rozstrzyga data dostarczenia przesyłki na adres Zamawiającego.
5. Każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt otrzymania wniosków, zawiadomień oraz informacji wysłanych za pośrednictwem faksu lub przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
6. Zamawiający udostępnia dokumentację z postępowania na pisemny wniosek osoby zainteresowanej. Dokumentację z postępowania udostępnia się w wyznaczonym przez Zamawiającego terminie w obecności pracownika Zamawiającego.
7. Osobami uprawnionymi do porozumiewania się z Wykonawcami są:
   Małgorzata Rejniak - starszy inspektor
8. Oświadczenia i dokumenty Wykonawca składa w formie wymaganej przez powszechnie obowiązujące przepisy prawa, w szczególności PZP i akty wykonawcze.
9. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ.
10. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert, Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu składania wniosku, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
11. Zamawiający zamieści wyjaśnienia na stronie internetowej, na której udostępniono SIWZ.
12. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w rozdz. VIII pkt 10 SIWZ.
13. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
14. Wszelkie uzupełnienia, ustalenia, zmiany terminów, jak również pytania od Wykonawców wraz z wyjaśnieniami stają się integralną częścią Specyfikacji Istotnych Warunków Zamówienia i będą wiążące przy składaniu ofert.

IX. WYMAGANIA DOTYCZĄCE WADIUM.

Zamawiający nie żąda wniesienia wadium w przedmiotowym postępowaniu.

X. TERMIN ZWIĄZANIA OFERTĄ.

1. Wykonawca pozostaje związany ofertą przez okres 30 dni.
2. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.
3. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą zwrócić się do Wykonawcy o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

XI. OPIS SPOSOBU PRZYGOTOWANIA OFERTY.

1. Ofertę należy złożyć na formularzu oferty stanowiącym Załącznik Nr 2 do SIWZ. Dokument musi być podpisany przez osobę uprawnioną do reprezentowania Wykonawcy.
2. Do oferty muszą być ponadto dołączone dokumenty wymienione w rozdziale VII ust. 1-4.
3. Ofertę należy sporządzić w języku polskim, czytelnie z zachowaniem formy pisemnej.
4. Oferta musi być umieszczona w kopercie zabezpieczonej przed otwarciem, posiadać nazwę i adres Wykonawcy oraz Zamawiającego oraz napis: „Oferta na zakup oprogramowania antywirusowego". Znak sprawy: KPB-V.273.29.2019. Nie otwierać przed 20 września 2019 r. godz. 11^{00}".

   UWAGA! W przypadku braku na kopercie ww. informacji, Zamawiający nie ponosi odpowiedzialności za zdarzenia mogące wyniknąć z powodu tego braku, np. przypadkowe otwarcie oferty przed wyznaczonym terminem, a w przypadku składania ofert pocztą lub pocztą kurierską – jej nie otwarcie w trakcie czynności otwarcia ofert.
5. Oferty przesłane pocztą należy umieścić w dodatkowej zewnętrznej kopercie i wysłać na adres: „Łódzki Urząd Wojewódzki w Łodzi, Biuro Kadr, Płac i Budżetu, 90 – 926 Łódź, ul. Piotrkowska 104, bud. „E", pok. 133", z tym, że za datę złożenia oferty przyjmowana będzie data wpływu oferty zgodnie z rozdziałem XII.1. i XII.2. SIWZ.
6. Każdy z Wykonawców może złożyć tylko jedną ofertę.
7. Wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane przez osobę podpisującą ofertę.
8. W przypadku, gdy ofertę (formularz oferty oraz wszystkie dokumenty) podpisuje lub potwierdza za zgodność z oryginałem inna osoba (osoby) niż uprawniona do reprezentowania Wykonawcy na podstawie aktualnego wpisu do właściwego rejestru, należy załączyć do oferty stosowne pełnomocnictwo lub upoważnienie. Pełnomocnictwo szczególne należy złożyć w formie oryginału, natomiast pełnomocnictwo ogólne należy złożyć w formie oryginału lub kserokopii potwierdzonej notarialnie za zgodność z oryginałem.
9. Potwierdzenie dokumentu za zgodność z oryginałem musi zawierać sformułowanie „Za zgodność z oryginałem" lub podobne oraz podpis i pieczęć imienną osoby uprawnionej do reprezentowania Wykonawcy, (jeśli Wykonawca się nią posługuje lub w przypadku jej braku czytelny podpis) lub inny podpis umożliwiający identyfikację osoby uprawnionej do reprezentowania Wykonawcy – na każdej zapisanej stronie dokumentu.
10. W przypadku złożenia oferty przez konsorcjum – należy do oferty dołączyć umowę konsorcjum w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem przez osobę uprawnioną do reprezentowania Wykonawcy.
11. Zaleca się, aby każda zapisana strona oferty była ponumerowana kolejnymi numerami, a cała oferta wraz z załącznikami była w trwały sposób ze sobą połączona, co uniemożliwiłoby jej samoistną dekompletację, oraz zawierała spis treści.
12. Ofertę należy przygotować tak, by z zawartością oferty nie można było zapoznać się przed upływem terminu otwarcia ofert.
13. Zamawiający żąda wskazania przez Wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez Wykonawcę firm podwykonawców. Informacje te zawiera Wykonawca w formularzu ofertowym.
14. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
15. Oświadczenia, o których mowa w rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 roku w sprawie rodzaju dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia publicznego (t.j. Dz. U. z 2016, poz. 1126) dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22a PZP oraz dotyczące podwykonawców, składane są w oryginale.
16. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentów, o których mowa w rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 roku w sprawie rodzaju dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia publicznego (t.j. Dz. U. z 2016, poz. 1126), innych niż oświadczenia, wyłącznie wtedy, gdy złożona kopia dokumentu jest nieczytelna lub budzi wątpliwości co do jej prawdziwości.

17. Jeżeli Wykonawca nie złoży oświadczeń, o których mowa w rozdz. VII SIWZ, oświadczeń lub dokumentów potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielenia wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania. Za wyjątkiem zapisów rozdziału VII ust. 10.
18. Jeżeli Wykonawca nie złoży wymaganych pełnomocnictw albo złoży wadliwe pełnomocnictwa, Zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
19. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.
20. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa", lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty. Brak jednoznacznego wskazania, które informacje stanowią tajemnice przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
21. Zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 1993 r. nr 47 poz. 2011 ze zmianami) będzie traktowane, jako bezskuteczne i skutkować będzie zgodnie z uchwałą Sądu Najwyższego z dnia 20 października 2005 roku (sygn. III CZP 74/05) potraktowaniem ich jako jawnych.
22. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 90 PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie Zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.
23. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty przed terminem składania ofert. Zmiana, poprawki lub modyfikacje treści oferty muszą zostać złożone wg takich samych zasad, jak składana oferta a ze złożonego oświadczenia musi jednoznacznie wynikać zamiar i zakres zmiany treści ofert. Zaleca się aby zmian treści oferty dokonać tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA". Koperty oznaczone „ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.
24. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia, według tych samych zasad jak wprowadzenie zmian i poprawek z napisem na kopercie „WYCOFANE". Koperty ofert wycofanych nie będą otwierane.
25. Do przeliczenia PLN wartości wskazanej w dokumentach złożonych na potwierdzenie spełnienia warunków udziału w postępowaniu, wyrażonej w walutach innych niż PLN, Zamawiający przyjmie średni kurs publikowany przez Narodowy Bank Polski zgodnie z powszechnie obowiązującymi przepisami prawa.
26. Wszelkie niejasności i obiekcje dotyczące treści zapisów w SIWZ należy wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym w rozdz. VIII pkt.10-11 SIWZ. Przepisy PZP nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów wzoru umowy, po terminie otwarcia ofert.

XII. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT.

1. Ofertę należy złożyć w siedzibie Zamawiającego, sekretariat Biura Kadr, Płac i Budżetu, ul. Piotrkowska 104, 90 – 926 Łódź, bud. „E", I p., pok. 133.
2. Termin składania ofert upływa dnia **20 września 2019 r. o godz. 10^{00}.**
3. Otwarcie ofert nastąpi w siedzibie Zamawiającego, ul. Piotrkowska 104, bud. „C", pok. 010.
4. Termin otwarcia ofert **20 września 2019 r. godz. 11^{00}.**

XIII. OPIS SPOSOBU OBLICZENIA CENY.

1. Wykonawca uwzględniając wszystkie wymogi, o których mowa w niniejszej Specyfikacji Istotnych Warunków Zamówienia, powinien w cenie brutto ująć wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania przedmiotu zamówienia uwzględniając inne opłaty i podatki, w tym koszty opakowania, ubezpieczenia, załadunku, rozładunku, transportu, spedycji, a także ewentualne upusty i rabaty zastosowane przez Wykonawcę.
2. Cenę oferty należy obliczyć w następujący sposób:
   1) podać cenę jednostkową netto danej pozycji (kol. 4);
   2) obliczyć wartość netto poprzez przemnożenie ilości przez jednostkową wartość netto (kol.3xkol.4);
   3) obliczyć cenę (łączną cenę netto wszystkich pozycji) poprzez zsumowanie cen netto poszczególnych pozycji;
   4) obliczyć wartość podatku VAT według stawki obowiązującej na dzień złożenia oferty;
   5) obliczyć cenę brutto poprzez zsumowanie ceny netto i wartości podatku VAT;
   6) ceny i wartości o których mowa w punktach 1 – 5 należy podać z dokładnością do dwóch miejsc po przecinku, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 grosza i wyższe zaokrągla się do 1 grosza.
3. Nie uwzględnienie przez Wykonawcę wszystkich kosztów nie będzie stanowić podstawy do domagania się ich pokrycia przez Zamawiającego w terminie późniejszym.
4. Obliczona przez Wykonawcę cena oferty powinna zawierać wszelkie koszty bezpośrednie i pośrednie jakie Wykonawca uważa za niezbędne do poniesienia dla prawidłowego wykonania przedmiotu zamówienia, zysk Wykonawcy oraz wszystkie wymagane przepisami podatki i opłaty. Wykonawca powinien uwzględnić w cenie wszystkie posiadane informacje o przedmiocie zamówienia, a w szczególności informacje, wymagania i warunki podane w niniejszej SIWZ.
5. Cena może być tylko jedna za oferowany przedmiot zamówienia, nie dopuszcza się wariantowości cen.
6. Cena nie ulega zmianie przez okres ważności oferty (związania ofertą).
7. Jeżeli cena oferty wydaje się rażąco niska w stosunku do przedmiotu zamówienia i budzi wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, w szczególności jest niższa o co najmniej 30% od wartości zamówienia powiększonej o należny podatek od towarów i usług ustalonej przed wszczęciem postępowania zgodnie z art. 35 ust. 1 i 2 ustawy Prawo zamówień publicznych lub średniej arytmetycznej cen wszystkich złożonych ofert Zamawiający zwraca się o udzielenie wyjaśnień, w tym złożenie dowodów, dotyczących elementów oferty mających wpływ na wysokość ceny.
8. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny, spoczywa na Wykonawcy.
9. Zamawiający poprawi w ofercie oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek.

XIV. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT, A JEŻELI PRZYPISANIE WAGI NIE JEST MOŻLIWE Z OBIEKTYWNYCH PRZYCZYN, ZAMAWIAJĄCY WSKAZUJE KRYTERIA OCENY OFERT W KOLEJNOŚCI OD NAJWAŻNIEJSZEGO DO NAJMNIEJ WAŻNEGO.

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

Kryterium	**Znaczenie kryterium**

1) **Cena** **60%**
2) **Termin realizacji zamówienia rozumiany jako dostawa i wdrożenie:** **40%**
   w tym:
   a) **dostawa w ciągu 14 dni** **0%**
   b) **dostawa w ciągu 10 dni** **20%**
   c) **dostawa w ciągu 7 dni** **40%**

Punkty wyliczane będą wg następującego wzoru:

1) **Cena (C)**

C = (cena najniższa : cena badana) x 100 pkt x 60%

Przez cenę Zamawiający rozumie łączną wartość brutto oferty.

2) **Termin realizacji (T)**
3) Ogólna punktacja:

P (punkty) = C + T

Wykonawca może zaoferować jeden z wymienionych powyżej okresów gwarancji licząc od dnia podpisania protokołu odbioru końcowego.

Zamawiający udzieli zamówienia Wykonawcy, który uzyska najwyższą liczbę punktów.

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

Po wyborze oferty najkorzystniejszej należy przedłożyć do wglądu, w przypadku złożenia oferty przez wspólników spółki cywilnej - umowę spółki w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem przez osobę uprawnioną do reprezentowania Wykonawcy

XVI. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie żąda zabezpieczenia należytego wykonania umowy w przedmiotowym postępowaniu.

XVII. 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.

1. Istotne dla Zamawiającego postanowienia, które zostaną wprowadzone do treści zawieranej umowy zawiera wzór umowy stanowiący Załącznik Nr 5 do SIWZ.
2. Umowa z Wykonawcą, którego oferta zostanie uznana za najkorzystniejszą, zostanie zawarta w terminie wyznaczonym przez Zamawiającego, w jego siedzibie w Łodzi przy ul. Piotrkowskiej 104.

XVIII. INNE INFORMACJE,

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Przedmiotem niniejszego postępowania nie jest zawarcie umowy ramowej.
3. Zamawiający nie przewiduje możliwości udzielania zamówień, których mowa w art. 67 ust. 1 pkt. 6 i 7 PZP.
4. Zamawiający nie dopuszcza składania ofert wariantowych zgodnie z art. 83 ust. 1 PZP.
5. Zamawiający nie przewiduje aukcji elektronicznej w niniejszym postępowaniu.
6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
7. Zamawiający nie przewiduje wymagań o których mowa w art. 29 ust. 3a PZP.
8. Zamawiający nie przewiduje wymagań, o których mowa w art. 29 ust. 4 PZP.
9. Zamawiający nie zamierza wykazywać obowiązku osobistego wykonywania przez Wykonawcę kluczowych części zamówienia.

10. Zamawiający nie określa standardów jakościowych, o których mowa w art. 91 ust. 2a PZP.
11. Zamawiający nie stawia wymogu oraz nie przewiduje możliwość złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty.

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

1. Wykonawcom przysługują środki ochrony prawnej przewidziane w Dziale VI PZP.
2. Środki ochrony prawnej określone w niniejszym dziale przysługują Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu tego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów PZP.
3. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym przez Prezesa Urzędu Zamówień Publicznych, na listę organizacji uprawnionych do wnoszenia środków ochrony prawnej.
4. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami PZP czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie PZP.
5. W niniejszym postępowaniu, odwołanie przysługuje wyłącznie 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.
6. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami PZP, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
7. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
8. 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.
9. 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, albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób.
10. Odwołanie wobec treści ogłoszenia o zamówieniu, a także wobec 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.
11. Odwołanie wobec czynności innych niż określone w ustępie 4 i 5 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.
12. Na orzeczenie Krajowej Izby Odwoławczej, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
13. Skargę wnosi się do sądu okręgowego właściwego dla siedziby Zamawiającego.
14. Skargę wnosi się za pośrednictwem Prezesa Izby w terminie 7 dni od dnia doręczenia orzeczenia Izby, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora publicznego jest równoznaczne z jej wniesieniem.

XX. Zastosowanie procedury uregulowanej w art. 24aa PZP.

1. Zamawiający może najpierw dokonać oceny ofert, a następnie zbadać, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

2. Jeżeli Wykonawca, o którym mowa w pkt. 1 uchyla się od zawarcia umowy, Zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu Wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert.

XXI. Klauzula informacyjna wynikająca z art. 13 Rozporządzenia RODO.

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 Wojewoda Łódzki. Siedzibą Wojewody Łódzkiego jest Łódzki Urząd Wojewódzki w Łodzi ul. Piotrkowska 104, 90-926 Łódź. Kontakt jest możliwy za pomocą telefonu: /42/ 664-10-00; adresu e-mail: kancelaria@lodz.uw.gov.pl; skrytki ePUAP: /lodzuw/skrytka.
2. W sprawach związanych z danymi osobowymi należy kontaktować się z Inspektorem ochrony danych poprzez adres e-mail: iod@lodz.uw.gov.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 na zakup oprogramowania antywirusowego, znak: **KPB-V.273.29.2019** prowadzonym w trybie przetargu nieograniczonego.
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 z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2018 r. poz. 1986 ze zm.), dalej „ustawa Pzp". Ponadto odbiorcami mogą być podmioty, które przetwarzają Pana/Pani dane osobowe w imieniu Administratora, na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (tzw. podmioty przetwarzające).
5. 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. Ponadto przez wymagany przepisami prawa okres archiwizacji zgodny z kategorią archiwalną, wynikającą z Jednolitego rzeczowego wykazu akt organów zespolonej administracji rządowej w województwie i urzędów obsługujących te organy.
6. 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.
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO.
8. Posiada Pani/Pan:
   1) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   2) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
   3) 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 **;
   4) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
9. Nie przysługuje Pani/Panu:
   1) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   2) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   3) 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.

---

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

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

Załączniki:

Nr 1 – szczegółowy opis przedmiotu zamówienia,
Nr 2 – formularz oferty,
Nr 3 – oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu,
Nr 4 – oświadczenie Wykonawcy dotyczące przesłanek wykluczenia z postępowania,
Nr 5 – wzór umowy,
Nr 6 – oświadczenie Wykonawcy – (grupa kapitałowa),

Załącznik Nr 1do SIWZ

Szczegółowy opis przedmiotu zamówienia.

Dostawa i wdrożenie oprogramowania antywirusowego.

Oprogramowanie antywirusowe ESET Endpoint Antivirus Suite przeznaczone na: stacje robocze, urządzenia mobilne oraz serwery (przedłużenie licencji na 700 sztuk oraz zakup dodatkowych licencji 500 sztuk, wraz z aktualizacją konsoli administracyjnej oraz klientów do najnowszej dostępnej wersji)
–**okres licencjonowania 3 lata**

lub równoważne, przy spełnieniu następujących wymagań:

- Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10.
- Wsparcie dla 32-bitowej i 64-bitowej wersji systemu Windows.
- Wersja programu dla stacji roboczych Windows oraz urządzeń mobilnych dostępna zarówno w języku polskim jak i angielskim.
- Pomoc w programie (help) i dokumentacja do programu w języku polskim.
- Wdrożenie oprogramowania wraz z przeszkoleniem administratorów (minimum 5 osób) w zakresie użytkowania, zarządzania oraz administrowania programem (czas trwania szkoleń - minimum: 16h) musi być przeprowadzone maksymalnie w ciągu 2 tygodni od podpisania umowy w siedzibie Zamawiającego.

Ochrona przed szkodliwym oprogramowaniem

- Wykrywanie szkodliwego oprogramowania, w szczególności: wirusów, makrowirusów, robaków internetowych, koni trojańskich, spyware, adware.
- Usuwanie wirusów, robaków internetowych, 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 oprogramowanie tego typu.
- Wbudowana technologia do ochrony przed rootkitami.
- Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
- Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

- Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
- Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
- Możliwość skanowania dysków sieciowych i dysków przenośnych.
- Skanowanie plików spakowanych i skompresowanych.
- Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
- Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej oraz lokalizacji pliku.
- Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
- Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
- Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
- Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
- Wbudowany konektor dla programów MS Outlook, Windows Mail i Windows Live Mail.
- Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Windows Mail i Windows Live Mail.
- Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
- Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
- Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
- Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
- Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
- Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
- Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych

protokołów HTTPS, POP3S, IMAPS.

- Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
- Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
- Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
- Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
- Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
- W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
- Wbudowane dwa niezależne moduły heurystyczne. Jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
- Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
- Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
- Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
- Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
- Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
- Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
- Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
- Program ma mieć możliwość definiowania typu aktualizacji systemowych, o braku których będzie informował użytkownika. Ma być możliwość dezaktywacji tego mechanizmu.

- Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
- System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
- System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
- Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych USB i SSD, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM.
- Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
- Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
- Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
- W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
- Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
- Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
- Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach,
    - tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
- Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

- Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
- Program musi posiadać zaawansowany skaner pamięci.
- Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
- Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
- Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
- Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
- Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
- Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
- Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http.
- Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
- Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
- Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
- W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
- Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
- Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
- Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
- Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych

- Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
- Wsparcie techniczne do programu musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona urządzeń mobilnych opartych o system Android:

- Ochrona i wsparcie systemów operacyjnych Android w wersji 4.x i wyższych.
- Ochrona plików w czasie rzeczywistym.
- Ochrona przed atakami typu „phishing".
- Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
- Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
- Ochrona proaktywna wykrywająca nieznane zagrożenia.
- W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
- Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
- Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
- Informacje o skanowaniu mają być przechowywane w plikach dziennika.
- Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
- Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.
- Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
- Dodanie zaufanej karty SIM ma się odbyć w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o wprowadzony ręcznie numer IMSI karty SIM.
- W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowanie urządzenia, uruchomienie sygnału dźwiękowego lub lokalizację GPS.
- Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej: połączenie Wi-Fi, GPS, usługi lokalizacyjne, pamięć, roaming danych, roaming połączeń, nieznane źródła, tryb debugowania, komunikacja NFC, szyfrowanie pamięci masowej oraz urządzenie zrootowane.
- Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
- Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
- Blokowanie aplikacji musi być możliwe w oparciu o: nazwę aplikacji, nazwę pakietu,

kategorię sklepu Google Play, uprawnienia aplikacji lub pochodzenie aplikacji z nieznanego źródła.

- W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej: minimalny poziom zabezpieczeń i złożoność blokady ekranu, maksymalną dopuszczaną liczbę błędnych prób odblokowania, odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie, czas, po którym automatycznie nastąpi blokada ekranu bądź ograniczenie dostępu do kamery wbudowanej w urządzenie.
- Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
- Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur.
- Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.
- Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
- Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
- Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
- Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.
- Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów: za pomocą kodu QR, za pomocą unikatowego łącza lub za pomocą wiadomości e-mail.
- Wsparcie techniczne do programu musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona serwerów Linux

- Skaner antywirusowy, antyspyware.
- Możliwość skanowania wszystkimi modułami programu (heurystyka, sygnatury, adware/spyware, aplikacje niepożądane, aplikacje niebezpieczne)
- Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail.
- Konfiguracja wszystkich modułów oprogramowania ma być możliwa poprzez edycję jednego pliku konfiguracyjnego.
- Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby warstw kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, maksymalnego rozmiaru archiwum samorozpakowującego, rozszerzenia skanowanego pliku.
- Możliwość skanowania podkatalogów oraz podążania za łączami symbolicznymi (symlinkami) w systemie.
- Możliwość definicji maksymalnego poziomu głębokości skanowanych podkatalogów.

- Możliwość tworzenia kwarantanny dla plików zainfekowanych w dowolnej lokalizacji w systemie plików.
- Możliwość zdefiniowania częstotliwości aktualizacji programu.
- Brak potrzeby instalacji dodatkowych zależności do systemu oprócz biblioteki LIBC, oprogramowanie po instalacji jest od razu gotowe do pracy.
- Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie.
- Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie.
- Wsparcie dla integracji oprogramowania z modułem Dazuko Access Controll (DAC) który odpowiada za skanowania plików w trybie on-access podczas zdarzeń typu otwarcie, zamknięcie oraz wykonanie pliku.
- Wsparcie dla skanowania za pośrednictwem biblioteki współdzielonej LIBC, która umożliwia skanowanie plików które są otwierane, zamykane lub wykonywane przez serwery plików (ftp, Samba) które wykorzystują zapytania do biblioteki LIBC.
- Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących.
- Możliwość tworzenia różnych akcji (przynajmniej 5-ciu różnych) w zależności od typu zdarzenia (w przypadku pliku nie przeskanowanego, pliku przeskanowanego, pliku zainfekowanego).
- Logowanie wykonanych akcji na plikach oraz zdarzeń dla poszczególnych modułów oprogramowania.
- Wsparcie dla zewnętrznego serwera logującgo syslog, możliwość definiowania dowolnego pliku logu (np. daemon, mail, user itp.).
- Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę Web.
- Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację i przeskanowanie dowolnego obszaru systemu plików a także przegląd statystyk dotychczas przeskanowanych plików.
- Interfejs programu dostępny przez przeglądarkę Web wykorzystuje wbudowany w program serwer http.
- Możliwość uruchomienia interfejsu Web na dowolnym interfejsie sieciowym
- Możliwość zabezpieczenia dostępu do interfejsu Web poprzez zdefiniowanie nazwy użytkownika i hasła.
- Interfejs Web ma przedstawić administratorowi dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy.
- Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu Web która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz pełną nazwę produktu którego dotyczy licencja.
- Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu Web. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie.
- Możliwość tworzenia osobnych ustawień skanowania dla poszczególnych użytkowników w systemie.

- Możliwość definicji użytkownika systemowego z prawami którego zostanie uruchomiony demon skanujący.
- Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta.
- Wysyłka podejrzanych plików ma być możliwa bezpośrednio do producenta lub za pośrednictwem serwera zdalnego zarządzania.
- Możliwość instalacji na dowolnym systemie Linux 2.6.x i nowszym.
- Możliwość instalacji na systemie FreeBSD 6.x, 7.x i 8.x i 9.x.
- Wsparcie dla platform 32 oraz 64 bitowych.
- Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych.
- System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail.
- Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwia prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego w jakim oprogramowanie zostało zainstalowane.
- Wsparcie techniczne do programu musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona serwerów Windows

- Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016).
- Wykrywanie szkodliwego oprogramowania, w szczególności: wirusów, makrowirusów, robaków internetowych, koni trojańskich, spyware, adware.
- Usuwanie wirusów, robaków internetowych, 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 oprogramowanie tego typu.
- Wbudowana technologia do ochrony przed rootkitami.
- Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
- Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
- System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.

- System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
- Możliwość skanowania dysków sieciowych i dysków przenośnych.
- Skanowanie plików spakowanych i skompresowanych.
- Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń).
- Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
- Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
- Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach,
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika.
- Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego
- Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
- Oprogramowanie musi posiadać zaawansowany skaner pamięci.
- Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
- Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
- Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
- Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych USB i SSD, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM.
- Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
- Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
- System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i

tworzyć dla nich odpowiednie wyjątki.

- Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
- Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
- Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
- Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
- W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
- Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
- System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
- Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
- Wbudowane dwa niezależne moduły heurystyczne. Jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
- Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
- Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
- Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
- Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
- W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez email.
- Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
- Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
- System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
- System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika.

- Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
- System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
- System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
- Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
- System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
- System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
- Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
- Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
- Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
- Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
- Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
- System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
- Aplikacja musi wspierać skanowanie magazynu Hyper-V.
- Praca programu musi być niezauważalna dla użytkownika.
- Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
- Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych
- Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet
- Wsparcie techniczne do programu musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Ochrona bezagentowa maszyn wirtualnych

- Rozwiązanie zapewnia bezagentową ochronę maszyn wirtualnych w wersjach systemu

gościa: Windows Server 2003 SP2 x32, Windows 7 x32/x64, Windows Server 2008 x32/x64, Windows Server 2008 R2 x32/x64, Windows Server 2012, Windows Server 2012 R2, Windows 8 x32/x64, Windows 8.1 x32/x64, Windows 10 x32/x64.

- Rozwiązanie umożliwia ochronę nieograniczonej liczby fizycznych serwerów ESXi w roli hypervisora.
- Ochrona środowiska wirtualnego zarządzana z jednej, centralnej konsoli administracyjnej, niezależnie od ilości chronionych hostów wirtualnych i serwerów w roli hypervisora.
- W ramach całego chronionego środowiska wirtualnego wymagane jest uruchomienie tylko jednej maszyny wirtualnej.
- Wyłączenie serwera z centralną konsolą administracyjną, nie wpływa na działanie mechanizmów ochrony maszyn wirtualnych (silniki antywirusowe pozostają aktywne).
- Wdrożenie rozwiązania do ochrony środowiska wirtualnego jest przeprowadzane w sposób zautomatyzowany z wykorzystaniem dedykowanego narzędzia, niezależnie od liczby systemów wirtualnych.
- Wdrożenie rozwiązania nie wymaga instalowania jakichkolwiek zewnętrznych składników czy plug-inów na natywnym systemie operacyjnym nadzorcy wirtualnego (hypervisora).
- Rozwiązanie funkcjonuje bez konieczności instalowania jakiegokolwiek własnego agenta na systemach operacyjnych wirtualnych hostów.
- Rozwiązanie wspiera środowisko VMware vSphere 5.5 U2 lub nowsze wraz z VMware NSX 6.2.4
- Ochrona środowiska wirtualnego realizowana jest z wykorzystaniem VMWare EPSec Library.
- Ochrona środowiska wirtualnego sprzedawana wraz z dwoma możliwymi do wyboru modelami licencjonowania: liczba chronionych hypervisorów lub liczba procesorów serwera hypervisora.
- Ochrona środowiska wirtualnego dostarczana jest wyłącznie w postaci obrazów maszyn wirtualnych (OVA- Open Virtual Appliance).
- Rozwiązanie wspiera technologię Vmware vMotion Migration - host wirtualny jest chroniony w trybie ciągłym niezależnie od tego na jakim serwerze fizycznym znajduje się w ramach jednego środowiska vSphere.
- System ochrony maszyny wirtualnej działa w trybie aktywnym (ochrona systemu w czasie rzeczywistym) jak i pasywnym (realizowanie skanowania na żądanie).
- Mechanizmy ochrony wirtualnych serwerów i desktopów realizowane są bezagentowo przez silnik producenta uruchomiony na dedykowanym wirtualnym appliance.
- Aktualizacje baz sygnatur antywirusowych pobierane są wyłączenie przez silnik producenta uruchomiony na dedykowanym wirtualnym appliance.
- Silnik antywirusowy wykorzystuje mechanizmy weryfikowania w chmurze producenta plików i procesów w czasie rzeczywistym - musi istnieć możliwość zdecydowania, czy funkcja ta ma być włączona, czy też nie.
- Do mechanizmów ochrony maszyn wirtualnych rozwiązanie wykorzystuje wyłączenie sieć zdefiniowaną programowo (SDN).
- Wyłączenie adaptera sieci TCP/IP na maszynie wirtualnej w żaden sposób nie wpływa na jej ochronę przez silnik antywirusowy.
- Administrator ma możliwość zdefiniowania aktywacji ochrony bezagentowej tylko na wybranych maszynach wirtualnych.

Administracja zdalna

- Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2008 R2, 2012, 2016, 2019 oraz systemach Linux.
- Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
- Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
- Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
- Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
- Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
- Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
- Interfejs może być zabezpieczony za pośrednictwem protokołu SSL.
- Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
- Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
- Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
- Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
- Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
- Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi, host agenta wirtualnego.
- Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, Linux, Android.
- Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
- Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
- Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
- Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji

podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich z możliwością jego odinstalowania.

- Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
- Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
- Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
- Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
- Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
- Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
- Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
- Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
- Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
- Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
- Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
- Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
- Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
- Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
- Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
- Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.

- Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
- Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
- Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
- Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
- Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
- Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV.
- Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
- Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
- Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
- Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
- Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
- W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
- Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
- Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
- Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
- Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
- W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
- Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
- Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.

- Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.

Załącznik Nr 2 do SIWZ
Załącznik Nr 1 do Umowy

.....
(pieczęć Wykonawcy) [*1]

Łódzki Urząd Wojewódzki w Łodzi
ul. Piotrkowska 104
90 – 926 Łódź

FORMULARZ OFERTY.
do sprawy: KPB-V.273.29.2019

Przystępując jako Wykonawca do postępowania o udzielenie zamówienia publicznego na zakup oprogramowania antywirusowego, składam następującą ofertę:

I. **Opis oferowanych urządzeń z podaniem nazwy producenta, modelu oraz typu, umożliwiający ich porównanie z wymaganiami określonymi w Załączniku Nr 1 do SIWZ**

Przedmiot zamówienia - oprogramowanie antywirusowe	**Nazwa oprogramowania**	**Ilość**
Typ zaoferowanego oprogramowania – przedłużenie licencji–**okres licencjonowania 3 lata**		700
Typ zaoferowanego oprogramowania – zakup licencji–**okres licencjonowania 3 lata**		500

II. Szczegółowy wykaz cen.

Oferuję przedmiot zamówienia za cenę:

Lp.	**Przedmiot zamówienia**	**Ilość**	**Cena netto dla 1 szt.**	**Wartość netto (kol. 3 x kol. 4)**
1.	2.	3.	4.	5.
1	Oprogramowanie antywirusowe ESET Endpoint Antivirus Suite lub równoważne - przedłużenie licencji **– okres licencjonowania 3 lata**	700		
2	Oprogramowanie antywirusowe ESET Endpoint Antivirus Suite lub równoważne - zakup licencji– **okres licencjonowania 3 lata**	500		
		SUMA:		

..... zł netto

..... zł podatek VAT

..... zł brutto

(słownie złotych: ..... brutto).

Termin realizacji zamówienia rozumiany jako dostawa i wdrożenie: …… dni.
*[2] *Wykonawca może zaoferować jeden z następujących terminów realizacji zamówienia: 14 dni, 10 dni, 7 dni.*

Oświadczam, że:

- zaoferowany przedmiot zamówienia spełnia wszystkie wymagania zawarte w Szczegółowym Opisie Przedmiotu Zamówienia (Załącznik Nr 1do SIWZ)

- zrealizuję przedmiot zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego w Specyfikacji Istotnych Warunków Zamówienia;
- wykonam przedmiot zamówienia w zadeklarowanym wyżej terminie
- w cenie oferty zostały uwzględnione wszelkie koszty wykonania zamówienia;
- zapoznałem się ze Specyfikacją Istotnych Warunków Zamówienia oraz wzorem umowy i nie wnoszę do nich zastrzeżeń oraz przyjmuję warunki w nich zawarte;
- uważam się za związany niniejszą ofertą na okres 30 dni licząc od dnia otwarcia ofert (włącznie z tym dniem);
- uzyskałem wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty;
- w przypadku wyboru mojej oferty do realizacji zamówienia podpiszę umowę w terminie wskazanym przez Zamawiającego;
- zamierzam powierzyć podwykonawcom następujące części zamówienia:

.....

.....

Dane kontaktowe Wykonawcy:

1. Adres: ……

2. Fax/tel: …….....

3. E-mail: ……..

4. NIP: ……...

5. REGON: ……...

Oświadczenie dotyczące wielkości przedsiębiorstwa:

- mikroprzedsiębiorstwo □

- małe przedsiębiorstwo□

- średnie przedsiębiorstwo□

- inne - duże □□

a) mikroprzedsiębiorstwem – przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.

b) małe przedsiębiorstwo – przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.

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

*** (Należy zakreślić właściwą kategorię. Te informacje są wymagane wyłącznie do celów statystycznych)**

Zastrzeżenia Wykonawcy

Niżej wymienione dokumenty składające się na ofertę nie mogą być ogólnie udostępnione:

……
……
……

Inne informacje Wykonawcy

1) ofertę niniejszą składam na …… kolejno ponumerowanych stronach,

2) wraz z ofertą składam następujące oświadczenia i dokumenty:
……
……
……
……

3) Wykonawca informuje, iż oświadczenia i/lub dokumenty składał, w postępowaniu prowadzonym przez Zamawiającego (należy podać znak sprawy tego postępowania):
……

4) Wykonawca informuje, iż Zamawiający może uzyskać wymagane dokumenty za pomocą bezpłatnych i ogólnie dostępnych baz danych pod adresem:
…….

Oświadczenie dotyczące danych osobowych:

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

....
(data) *(podpis i pieczęć imienna)* *[3]

*[1] - odcisk pieczęci firmowej, jeśli Wykonawca się nią posługuje lub pełna nazwa Wykonawcy;
*[2]- należy wybrać jeden z podanych terminów realizacji;
*[3]- podpis i pieczęć imienna, jeśli Wykonawca się nią posługuje lub w przypadku jej braku czytelny podpis.

Załącznik Nr 3 do SIWZ

.....

(nazwa Wykonawcy)[*1]

O Ś W I A D C Z E N I E
o spełnieniu warunków udziału w postępowaniu*
wymagane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych
(t.j. Dz.U. z 2018 r., poz. 1986)
KPB-V.273.29.2019

Przystępując jako Wykonawca do postępowania o udzielenie zamówienia publicznego na zakup oprogramowania antywirusowego.

oświadczam, że:

- spełniam warunki udziału w postępowaniu określone przez Zamawiającego

....
(data) *(podpis i pieczęć imienna)*[*2]

Informacja w związku z poleganiem na zasobach innych podmiotów:

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

…….

..……..…

……., w następującym zakresie: …….

……...

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

....
(data) *(podpis i pieczęć imienna)*[*2]

*** Wykonawca składa niniejsze oświadczenie wyłącznie jeżeli Zamawiający sformułował warunki udziału w postępowaniu w SIWZ.**

Oświadczenie dotyczące podanych informacji:

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

....

(data) *(podpis i pieczęć imienna)*[*2]

[*1] – odcisk pieczęci firmowej, jeśli Wykonawca się nią posługuje lub pełna nazwa Wykonawcy;
[*2] – podpis i pieczęć imienna, jeśli Wykonawca się nią posługuje lub w przypadku jej braku czytelny podpis.

Załącznik Nr 4 do SIWZ

.....
(pieczęć Wykonawcy) [*1]

OŚWIADCZENIE
dotyczące przesłanek wykluczenia z postępowania
wymagane na podstawie art. 25a ust. 1
ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
(t.j. Dz.U. z 2018 r., poz. 1986 ze zm.)

do sprawy KPB-V.273.29.2019

Przystępując jako Wykonawca do postępowania o udzielenie zamówienia publicznego na zakup oprogramowania antywirusowego.

Jako Wykonawca oświadczam, że:

1) nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-23 ustawy.
2) nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust. 5 pkt 1 ustawy.

....
(data) *(podpis i pieczęć imienna)* [*2]

Jako Wykonawca oświadczam, że:

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

……..
……..…….....
..……
……...

....
(data) *(podpis i pieczęć imienna)* [*2]

Oświadczenie dotyczące podmiotu, na którego zasoby powołuje się Wykonawca:

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: …….

……...

……...

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

....

(data) *(podpis i pieczęć imienna)*[*2]

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

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

……..……

……...

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG),

nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

....

(data) *(podpis i pieczęć imienna)*[*2]

Oświadczenie dotyczące podanych informacji:

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

....

(data) *(podpis i pieczęć imienna)*[*2]

*[1] – odcisk pieczęci firmowej, jeśli Wykonawca się nią posługuje lub pełna nazwa Wykonawcy;
*[2] – podpis i pieczęć imienna, jeśli Wykonawca się nią posługuje lub w przypadku jej braku czytelny podpis.

Załącznik Nr 5 do SIWZ

KPB-V.273.29.2019

Wzór Umowy

zawarta w dniu ..... w Łodzi, na mocy zgodnego porozumienia stron, pomiędzy:

Skarbem Państwa – Łódzkim Urzędem Wojewódzkim w Łodzi z siedzibą w Łodzi przy ul. Piotrkowskiej 104, 90 – 926 Łódź, NIP 725-10-28-465, REGON: 004 308 002 reprezentowanym przez Pana Mirosława Suskiego - Dyrektora Generalnego Urzędu, zwanym w dalszej części Umowy **„Zamawiającym”**
a
.....z siedzibą.....

reprezentowanym przez: ..... zwanym dalej **„Wykonawcą”**

Zamawiający i Wykonawca w dalszej części Umowy zwani są także „Stroną” lub „Stronami”

Umowa została zawarta po przeprowadzeniu postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, zgodnie z art. 10 ust. 1 oraz art. 39-46 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 ze zm.), w dalszej części Umowy jako „PZP”, postępowanie Nr KPB-V.273.29.2019.

§ 1
PRZEDMIOT UMOWY

1. Przedmiotem niniejszej Umowy jest dostawa do siedziby Zamawiającego i wdrożenie oprogramowania antywirusowego ESET Endpoint Antivirus Suite przeznaczonego na: stacje robocze, urządzenia mobilne oraz serwery (przedłużenie licencji na 700 sztuk oraz zakup dodatkowych licencji 500 sztuk, wraz z aktualizacją konsoli administracyjnej oraz klientów do najnowszej dostępnej wersji), dalej jako „Przedmiot Umowy”, wg zestawienia zawartego w opisie oferowanych urządzeń zawartym w formularzu oferty oraz w Szczegółowym Opisie Przedmiotu Zamówienia, stanowiących załącznik Nr 1 do Umowy.
2. Dostarczony Przedmiot Umowy musi być fabrycznie nowy, nieużywany, sprawny i nie może być przedmiotem praw ani zobowiązań osób trzecich.
3. Dostarczony Przedmiot Umowy pochodzić będzie z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.
4. Przejście na Zamawiającego ryzyka związanego z Przedmiotem Umowy następuje z chwilą podpisania przez strony Umowy protokołu odbioru, o jakim mowa w § 3 ust. 3.

§ 2
WYKONANIE PRZEDMIOTU UMOWY

1. Wykonawca zobowiązuje się wykonać Przedmiot Umowy zgodnie z obowiązującym w Rzeczypospolitej Polskiej prawem oraz obowiązującymi w Polsce normami technicznymi, zachowując przy tym należytą staranność.
2. Wykonawca zobowiązany jest dostarczyć tzw. dokumentację użytkownika dla Przedmiotu Umowy stanowiącą wytyczne dotyczące obsługi, w języku polskim lub angielskim, nośniki instalacyjne.
3. Wykonawca zobowiązany jest dokonać instalacji i wdrożenia dostarczonego oprogramowania na zasadach określonych przez strony.
4. Wykonawca gwarantuje, że usługi w ramach Umowy będą świadczone w sposób profesjonalny zgodnie ze standardami obowiązującymi w branży informatycznej.
5. Wykonawca oświadcza, że jest właścicielem autorskich praw majątkowych do oprogramowania stanowiącego Przedmiot Umowy oraz że jest podmiotem uprawnionym do udzielania licencji i dostawy ww. oprogramowania.
6. Przedmiotem Umowy jest udzielenie przez Wykonawcę na rzecz Zamawiającego licencji na oprogramowanie stanowiące przedmiot Umowy obejmującej prawo do korzystania przez Zamawiającego z Przedmiotu Umowy w zakresie i w sposób oraz okres określony w Szczegółowym Opisie Przedmiotu Zamówienia oraz w formularzu oferty stanowiącym Załącznik Nr 1.

§ 3
WARUNKI REALIZACJI DOSTAWY

1. Wykonawca, na koszt własny, dostarczy Przedmiot Umowy Zamawiającemu do jego siedziby.
2. Wykonawca zobowiązany jest zawiadomić Zamawiającego o gotowości do dostawy i montażu z wyprzedzeniem nie mniejszym niż 3 dni przed dostawą. Strony Umowy uzgodnią konkretny dzień dostawy i godziny (przedział czasowy), w jakich nastąpi dostarczenie Przedmiotu Umowy i jego odbiór.
3. Odbioru Przedmiotu Umowy, dokonają upoważnieni pracownicy Zamawiającego za protokołem odbioru. Dniem dostarczenia Przedmiotu Umowy jest dzień podpisania przez strony Umowy protokołu odbioru końcowego bez zastrzeżeń.
4. Jeżeli w trakcie odbioru stwierdzona zostanie wada Przedmiotu Umowy, Zamawiający może odmówić jego odbioru, a Wykonawca zobowiązany będzie, w zależności od wyboru Zamawiającego, do wymiany wadliwego Przedmiotu Umowy na wolny od wad, w terminie uzgodnionym protokolarnie przez strony Umowy, przy czym termin ten nie może być dłuższy niż 14 dni roboczych od dnia poinformowania Wykonawcy o stwierdzeniu wady, bądź do usunięcia wady w drodze jego naprawy, w terminie uzgodnionym protokolarnie przez strony Umowy, przy czym termin ten nie może być dłuższy niż 7 dni roboczych od dnia poinformowania Wykonawcy o stwierdzeniu wady. W przypadku stwierdzenia braków ilościowych w dostawie, Wykonawca jest zobowiązany do ich uzupełnienia w terminie uzgodnionym protokolarnie przez strony Umowy, nie dłuższym jednak niż 7 dni roboczych od dnia stwierdzenia braków. Przez wadę rozumie się w szczególności jakąkolwiek niezgodność z opisem Przedmiotu Umowy określonego wg zestawienia zawartego w opisie oferowanych urządzeń zawartym w formularzu oferty, stanowiącym Załącznik nr 1 do Umowy.
5. Ze strony Zamawiającego, osobą uprawnioną do kontaktów w sprawie realizacji umowy z Wykonawcą jest: ……..
6. Ze strony Wykonawcy, osobą uprawnioną do kontaktów w sprawie realizacji umowy z Zamawiającym jest: ……
7. Fakturę VAT dokumentującą dostawę Przedmiotu Umowy należy wystawić – nie wcześniej niż po podpisaniu przez strony Umowy protokołu odbioru końcowego, o jakim mowa w § 3 ust. 3 na:
   Łódzki Urząd Wojewódzki w Łodzi,
   90-926 Łódź, ul. Piotrkowska 104,
   NIP 725-10-28-465, REGON 004308002

§ 4
TERMIN REALIZACJI

1. Wykonawca wykona Przedmiot Umowy w terminie … dni od dnia podpisania Umowy.
2. Dniem wykonania Przedmiotu Umowy jest dzień podpisania przez Strony Umowy protokołu odbioru końcowego określonego w § 3 ust. 3 bez zastrzeżeń.

§ 5
WYNAGRODZENIE

1. Zamawiający zapłaci Wykonawcy za wykonanie Przedmiotu Umowy, w tym za udzielenie licencji w zakresie określonym w niniejszej umowie cenę brutto: ..... PLN, słownie..... w tym kwota podatku VAT wynosi ……..…. PLN,
2. Wynagrodzenie podane w ust.1 jest zgodne ze złożoną ofertą i opisem oferowanych urządzeń oraz obejmuje wszystkie elementy cenotwórcze, wynikające z zakresu i sposobu realizacji Przedmiotu Umowy i które zostały określone w szczegółowym wykazie cen, stanowiącym **Załącznik Nr 2** do Umowy, w tym koszty opakowania, ubezpieczenia, załadunku, rozładunku, transportu, spedycji.
3. Podstawą do wystawienia przez Wykonawcę faktury za zrealizowanie Przedmiotu Umowy jest podpisany bez zastrzeżeń przez obie strony Umowy protokół odbioru końcowego określonego w § 3 ust. 3.
4. Zapłata wynagrodzenia objętego treścią faktury, o jakiej mowa w ust. 3, nastąpi przelewem w ciągu 14 dni od daty otrzymania prawidłowo wystawionej faktury, na rachunek bankowy Wykonawcy wskazany w jej treści.
5. Za dzień zapłaty wynagrodzenia Wykonawcy uważać się będzie dzień obciążenia rachunku Zamawiającego.
6. Ceny jednostkowe na fakturze VAT winny być zgodne z cenami z formularza ofertowego.

§ 6

WARUNKI GWARANCJI I RĘKOJMII

1. Wykonawca udziela gwarancji i wsparcia na oprogramowanie będące przedmiotem umowy przez czas trwania licencji określonej niniejszą umową.
2. W okresach gwarancji i wsparcia określonych w ust. 1 Wykonawca zapewni bezpłatne naprawy gwarancyjne i serwis Przedmiotu Umowy w siedzibie Zamawiającego oraz bezpłatne udzielenie konsultacji i pomocy technicznej w zakresie działania Przedmiotu Umowy.
3. Serwis gwarancyjny realizowany będzie przez producenta lub autoryzowanego partnera serwisowego producenta.
4. Zgłoszenia awarii dokonywane będą pisemnie, telefonicznie, faksem lub pocztą elektroniczną.
5. Strony dopuszczają możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną. W razie awarii dysków, dyski pozostają własnością Zamawiającego.
6. Wykonawca w ramach gwarancji jest zobowiązany podjąć naprawę awarii najpóźniej do końca następnego dnia roboczego od daty zgłoszenia i wykonać naprawę najpóźniej w terminie 14 dni od daty zgłoszenia usterki. Zgłoszenia przesłane po godzinach pracy serwisu traktowane będą jak wysłane w najbliższym dniu roboczym o godzinie otwarcia punktu serwisowego.
7. Uprawnienia wynikające z udzielonej gwarancji nie wyłączają możliwości dochodzenia przez Zamawiającego uprawnień z tytułu rękojmi za wady.
8. Wykonawca ponosi odpowiedzialność za wszelkie szkody wyrządzone podczas wykonywania zobowiązań Umowy.

§ 7

PODWYKONAWCY

1. Wykonawca, który w toku postępowania o udzielenie zamówienia publicznego, powoływał się na zasadach określonych w art. 22a ust. 1 PZP na zasoby innych podmiotów nie jest zwolniony z odpowiedzialności za należyte wykonanie tego zamówienia.
2. W przypadku zmiany albo rezygnacji, podmiotów o których mowa w ust. 1, w celu wykazania spełnienia warunków udziału w postępowaniu, o którym mowa w art. 22 ust. 1 PZP, Wykonawca jest obowiązany wykazać Zamawiającemu, iż proponowany inny Podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia.
3. Jeżeli Zamawiający stwierdzi, że wobec danego Podwykonawcy zachodzą podstawy wykluczenia, Wykonawca obowiązany będzie zastąpić tego Podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia Podwykonawcy.
4. W przypadku powierzenia przez Wykonawcę realizacji Przedmiotu Umowy Podwykonawcom, Wykonawca zobowiązany będzie do niezwłocznego poinformowania o tym fakcie Zamawiającego.
5. Wykonawca będzie odpowiadał za działania lub zaniechania Podwykonawców jak za własne.

§ 8

KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu kary umowne z następujących tytułów:
   1) za opóźnienie w dostawie części lub całości Przedmiotu Umowy – w wysokości 2 % wynagrodzenia brutto, o jakim mowa w § 5 ust. 1, za każdy dzień opóźnienia, liczony od dnia następnego przypadającego po dniu, w którym zgodnie z Umową miała nastąpić dostawa,
   2) za opóźnienie w wykonaniu zobowiązań z tytułu gwarancji lub rękojmi – w wysokości 1 % wynagrodzenia brutto, o jakim mowa w § 5 ust. 1, za każdy dzień opóźnienia, liczony od dnia następnego przypadającego po dniu, w którym zobowiązanie miało zostać wykonane,
   3) w wysokości 10 % wynagrodzenia brutto, o jakim mowa w § 5 ust. 1 w przypadku odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy.
2. Wykonawca nie ponosi odpowiedzialności za opóźnienia lub nie dojście do skutku dostawy, jeżeli jest to wywołane "siłą wyższą".
3. Jako „siły wyższe” uznane zostają: klęski żywiołowe, huragan, powódź, katastrofy transportowe, pożar, eksplozje, wojna, strajk i inne nadzwyczajne wydarzenia, których zaistnienie leży poza zasięgiem i kontrolą układających się Stron.
4. Zamawiający jest uprawniony do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych w przypadku, gdy szkoda przewyższa wartość zastrzeżonych kar umownych.
5. Wykonawca wyraża zgodę na potrącenie przez Zamawiającego kary umownej z wynagrodzenia

przysługującego Wykonawcy z tytułu Umowy.

§ 9

ODSTĄPIENIE OD UMOWY / ROZWIĄZANIE UMOWY

W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania - do dnia odstąpienia - części Umowy.

§ 10

DANE OSOBOWE

1. Wykonawca oświadcza, że wypełnił obowiązki informacyjne przewidziane w art. 13 i art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 roku, s. 1) RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu realizacji niniejszej Umowy.
2. Obowiązek informacyjny stanowi **Załącznik Nr 3**.

§ 11

POSTANOWIENIA KOŃCOWE

1. Wszelkie spory powstałe na tle stosowania Umowy będą rozstrzygane polubownie. W przypadku braku porozumienia, właściwym do rozpoznawania spraw spornych będzie sąd właściwy dla siedziby Zamawiającego.
2. Wszelkie zmiany i uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych Umową mają zastosowanie przepisy Kodeksu cywilnego, PZP oraz powszechnie obowiązujące przepisy prawa.
4. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, na prawach oryginału każdy, dwa dla Zamawiającego i jeden dla Wykonawcy.

Załączniki:
Nr 1 - kopia formularza oferty w zakresie opisu oferowanych urządzeń i szczegółowego opisu przedmiotu zamówienia,
Nr 2 - kopia formularza oferty w zakresie szczegółowego wykazu cen,
Nr 3 - obowiązek informacyjny.

Zamawiający **Wykonawca**

Załącznik nr 3 do umowy
Nr KPB-V.273.29.2019 r.
z dnia ……

Obowiązek informacyjny

Obowiązek informacyjny zostanie przedstawiony Wykonawcy w dniu podpisania umowy.

Załącznik nr 6 do SIWZ

O Ś W I A D C Z E N I E
dotyczące przynależności lub braku przynależności do tej samej grupy kapitałowej
zgodnie z art. 24 ust. 1 pkt. 23 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
(t.j. Dz.U. z 2018 r., poz. 1986 ze zm.)

do sprawy KPB-V.273.29.2019

*Należę / Nie należę**[2]
do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r., poz. 369).

*Przedstawiam/nie przedstawiam**[2]
dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia

Jako dowody załączam: …….

....
(data) *(podpis i pieczęć imienna)**[3]

*[1] – odcisk pieczęci firmowej, jeśli Wykonawca się nią posługuje lub pełna nazwa Wykonawcy;
[2] – niepotrzebne skreślić;[3] – podpis i pieczęć imienna, jeśli Wykonawca się nią posługuje lub w przypadku