SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Nazwa nadana zamówieniu: „***Dostawa oprogramowania antywirusowego wraz z konsolą do zarządzania. DP.2301.8.2019"***

Wartość zamówienia przekracza wyrażoną w złotych równowartości kwoty 221. 000 euro.

Oznaczenie sprawy: ***DP.2301.8.2019***

Ogłoszenie o niniejszym przetargu zostało zamieszczone:

- w Dzienniku Urzędowym Unii Europejskiej – dnia 19.02.2019r. pod numerem Dz.U. 2019/S 035-078294 : (wysłano do publikacji w dniu 14.02.2019r.)
- miniPortalu https://miniportal.uzp.gov.pl/ dnia 14.02.2019
- na stronie internetowej Zamawiającego www.ujk.edu.pl dnia 14.02.2019 r.
- na tablicy ogłoszeń w siedzibie Zamawiającego – dnia 14.02.2019 r.

ROZDZIAŁ I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Uniwersytet Jana Kochanowskiego w Kielcach
ul. Żeromskiego 5
25-369 Kielce
tel.: (041) 3497277 faks: (041) 3445615
Adres strony internetowej: www.ujk.edu.pl

Adres elektronicznej skrzynki podawczej ePUAP: /UJK/SkrytkaESP

ROZDZIAŁ II. TRYB UDZIELENIA ZAMÓWIENIA

Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone będzie w trybie przetargu nieograniczonego na podstawie art. 39 ustawy z dnia 29 stycznia 2004r. - Prawo zamówień publicznych (t.j. Dz. U. 2018 poz. 1986 ze zm.).zwanej dalej „PZP".
W zakresie nieuregulowanym niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ" zastosowanie mają przepisy ustawy PZP.
Postępowanie prowadzone jest **w oparciu o zapisy art. 24aa ustawy**, Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

ROZDZIAŁ III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. ***Przedmiotem zamówienia jest***

   Dostawa oprogramowania antywirusowego wraz z konsolą do zarządzania. Szczegółowy opis przedmiotu zamówienia, opis parametrów technicznych i dodatkowych wymagań, zostały opisane w załączniku nr 2 do niniejszej specyfikacji – opis przedmiotu zamówienia. Jeżeli dla danych pozycji zamawiający wskazał klasę, markę czy znak towarowy oprogramowania, to dopuszcza się zaoferowanie oprogramowania równoważnego pod warunkiem zachowania norm, konstrukcji, parametrów i standardów, którymi charakteryzuje się sprzęt wskazany przez zamawiającego. W tym wypadku na wykonawcy spoczywa obowiązek udowodnienia zachowania cech określonych w załączniku nr 2 do niniejszej specyfikacji tj. należy sporządzić i załączyć specyfikację techniczną oferowanego sprzętu jako załącznik do formularza ofertowego. W przeprowadzonym dowodzie należy odnieść się do norm, konstrukcji, parametrów oraz standardów i dokonać porównania, z którego musi wynikać, iż sprzęt oferowany jako równoważny jest identyczny lub lepszy od sprzętu wskazanego przez zamawiającego.

2. ***Kod CPV:***

   48620000 – 0 systemy operacyjne

   48000000 – 0 pakiety oprogramowania i systemy informatyczne

3. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych we wzorze umowy stanowiącym załącznik nr 3 do SIWZ.

4. **Wykonawca zobowiązany będzie do:**

- przeszkolenia pracowników zamawiającego z zakresu obsługi dostarczonego oprogramowania– zgodnie z treścią opisu przedmiotu zamówienia tj. jednodniowe szkolenie techniczne dla co najmniej 15 administratorów w siedzibie Zamawiającego.

- Instalacji systemu antywirusowego w siedzibie zamawiającego w terminie uzgodnionym z Zamawiającym.

- Jednodniowa asysta inżyniera Wykonawcy w wdrożeniu oprogramowania antywirusowego wraz z wdrożeniem całego systemu zarządzania - uruchomienie konsoli zarządzającej oprogramowaniem antywirusowym.

- Asysta przy migracji do nowego systemu antywirusowego – co najmniej 8 godzin.

- Wsparcie techniczne : bezpłatna pomoc techniczna w okresie ważności licencji świadczona przez przeszkolonego inżyniera w języku polskim w dni robocze w godz. 8 -16.

- Bezpłatna aktualizacja baz sygnatur wirusów oraz zakupionego oprogramowania w okresie ważności licencji.

- Ważność licencji (pożądana) od 12.04.2019 r. kiedy wygasa licencja na poprzednie oprogramowanie antywirusowe

- świadczenia serwisu gwarancyjnego w okresie gwarancji w miejscu instalacji , na zasadach określonych w umowie.

5. Wymagany okres gwarancji i rękojmi na dostarczone oprogramowanie został określony w opisie przedmiotu zamówienia, w załączniku nr 1. (Oferty zawierające okres gwarancji i rękojmi krótszy niż wskazany w załączniku nr 1 zostaną odrzucone).

6. Wszystkie dokumenty załączone do dostarczonego przedmiotu zamówienia muszą być sporządzone w języku polskim w formie drukowanej (instrukcja obsługi dodatkowo na DVD, CD lub pendrive).

UWAGA:

W przypadku wystąpienia w SIWZ lub którymkolwiek załączniku do SIWZ nazw producenta, oprogramowanie można zastąpić równoważnym, które nie będzie gorsze niż to wskazane w SIWZ oraz gwarantować będzie zachowanie parametrów i funkcjonalności opisanych w SIWZ. Wykonawca, który powołuje się na rozwiązania równoważne jest obowiązany wykazać, że oferowany przez niego oprogramowanie spełnia wymagania określone przez zamawiającego. Ewentualne występujące w SIWZ nazwy (w tym nazwy własne, znaki towarowe i sformułowania „np.”), typy i pochodzenie produktów nie są dla wykonawcy wiążące i nie mają

na celu naruszenia art. 29 i art. 7 ustawy PZP, a jedynie doprecyzowanie oczekiwań jakościowych, funkcjonalnych i technologicznych zamawiającego. Wszystkie zmiany i odstępstwa nie mogą powodować obniżenia wartości funkcjonalnych i użytkowych oprogramowania oraz nie mogą powodować zmniejszenia jego trwałości eksploatacyjnej. Wszystkie planowane rozwiązania równoważne i zamienne muszą być uzgodnione pomiędzy zamawiającym a wykonawcą.

7. Zamawiający **nie dopuszcza składania ofert częściowych.**

8. Zamawiający **nie dopuszcza możliwości składania ofert wariantowych.**

10. Zamawiający **nie przewiduje udzielenia zamówienia na dodatkowych**

11. Zamawiający na podstawie art.36b. ust.1 żąda wskazania przez wykonawcę w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców (jeżeli są znani).

12. Zamawiający **nie przewiduje aukcji elektronicznej.**

13. Wykonawca **może powierzyć wykonanie części zamówienia podwykonawcy**.

Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.

14. Dostawę należy wykonać z zachowaniem szczególnej staranności, zgodnie z umową oraz niniejszą SIWZ.

ROZDZIAŁ IV. TERMIN REALIZACJI ZAMÓWIENIA

Termin wykonania zamówienia -3 lata od popisania umowy, ale nie wcześniej niż od **12.04.2019 r.** ,kiedy wygasa licencja na poprzednie oprogramowanie antywirusowe.

ROZDZIAŁ V. WARUNKI UDZIAŁU W POSTĘPOWANIU

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

1) **nie podlegają wykluczeniu;**

a) *art. 24 ust. 1 pkt 12–23 ustawy*

b) *art. 24 ust. 5 pkt 1)* tj, 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 (t.j. Dz.U.2016 poz. 1574) 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 2016 r. poz. 2171, 2260 i 2261 oraz z 2017 r. poz. 791);

2) **spełniają warunki udziału w postępowaniu dotyczące:**

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

Zamawiający nie określa wymagań w tym zakresie.

b) sytuacji ekonomicznej lub finansowej;

Zamawiający nie określa wymagań w tym zakresie.

c) zdolności technicznej lub zawodowej; Wykonawca spełni warunek, jeżeli wykaże, że:

- **w okresie ostatnich 3 lat przed upływem terminu składania ofert**, a jeżeli okres prowadzenia działalności jest krótszy- w tym okresie, wykonał należycie minimum trzy dostawy oprogramowania antywirusowego o minimalnej wartości 80.000,00 zł brutto każda (słownie złotych: osiemdziesiąt tysięcy 00/100).

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia wymagana ilość dostaw nie sumuje się.

1. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz pkt 16-20 lub ust. 5 pkt.1 ustawy PZP może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu Wykonawcy. Przepisu nie stosuje się, jeżeli wobec Wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.
2. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające dowody przedstawione na podstawie pkt 2.
3. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.
4. Wykluczenie Wykonawcy następuje zgodnie z art. 24 ust. 7 Pzp.
5. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

6. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
7. Zamawiający ocenia, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 12–23 ustawy oraz ust.5 pkt. 1.

9. Jeżeli zdolności techniczne lub zawodowe podmiotu, o którym mowa w pkt. 6, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tych podmiotów podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego:

1) zastąpił ten podmiot innym podmiotem lub podmiotami lub

2) zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe, o których mowa w pkt. 1. 2).

10. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a Pzp, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający wymaga, aby z treści ww. zobowiązania wynikało w szczególności:

- zakres dostępnych Wykonawcy zasobów innego podmiotu;
- sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego;
- zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego.
- czy inne podmioty, na zdolności, których wykonawca powołuje się w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizują roboty budowlane lub usługi, których wskazane zdolności dotyczą.

11. Wykonawca, który polega na zasobach innych podmiotów składa na wezwanie Zamawiającego dokumenty o których mowa w rozdziale VI pkt. 6.2 w odniesieniu do tych podmiotów.

12. Potwierdzenie spełnienia przez Wykonawcę warunków, o których mowa w pkt. 1 ppkt.2), nastąpi na podstawie przedłożonych przez Wykonawcę dokumentów i oświadczeń, wymienionych w Rozdziale VI.

ROZDZIAŁ VI. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW DO WYKLUCZENIA

1. **Do oferty wykonawca musi dołączyć:**

- aktualne na dzień składania ofert oświadczenie w zakresie wskazanym przez zamawiającego w niniejszej SIWZ. Oświadczenie składa się na formularzu Jednolitego Europejskiego Dokumentu Zamówienia (**JEDZ)**, sporządzonego zgodnie z wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE. Informacje zawarte w JEDZ będą stanowić wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Zarówno JEDZ jak i ofertę składa się wyłącznie w formie elektronicznej.

2. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie JEDZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokument ten ma wstępnie potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia.

3. W przypadku gdy wykonawca będzie polegał na zdolnościach lub sytuacji innych podmiotów, musi udowodnić zamawiającemu, że realizując zamówienie będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

4. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania – w zakresie w jakim powołuje się na ich zasoby – warunków udziału w postępowaniu składa także oświadczenie JEDZ dotyczące tych podmiotów.

Ponadto Wykonawca złoży:

a) **Pełnomocnictwo do reprezen**towania Wykonawcy w niniejszym postępowaniu lub/i do podpisania umowy (o ile nie wynika z dokumentów rejestracyjnych). Pełnomocnictwo musi być podpisane przez osoby uprawnione do reprezentowania Wykonawcy (kwalifikowalny podpis/podpisy osób udzielających pełnomocnictwa) lub mieć postać aktu notarialnego, albo notarialnie potwierdzonej kopii, lub kopii potwierdzonej za zgodność z oryginałem w sposób zgodny z Rozporządzeniem Ministra Rozwoju z dnia 27 lipca 2016r. w sprawie rodzajów dokumentów jakich

może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016r. poz.1126 ze zm.)

b) **Dowód wniesienia wadium** – jeżeli będzie wniesione w innej formie niż pieniężna.

c) **szczegółowe opisy oferowanego oprogramowania** antywirusowego ze szczególnym uwzględnieniem parametrów technicznych wraz z folderami producenta.

W przypadku wnoszenia oferty wspólnej przez dwa lub więcej podmioty gospodarcze (konsorcja/spółki cywilne) oferta musi spełniać wymagania określone w art. 23 ustawy Prawo zamówień publicznych.

5. Wykonawca w terminie **3 dni** od dnia zamieszczenia przez Zamawiającego informacji, o której mowa w art. 86 ust. 5 ustawy PZP, przekaże zamawiającemu ***oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej***, o której mowa w art. 24 ust. 1 pkt. 23 ustawy PZP- wzór oświadczenia stanowi załącznik nr 6 do SIWZ. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia publicznego. *W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia w/w oświadczenie składa każdy z Wykonawców. Oświadczenie musi być złożone w wersji elektronicznej i być podpisane kwalifikowalnym podpisem elektronicznym.*

6. Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, **nie krótszym niż 10 dni**, aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:

6.1 w celu potwierdzenia braku podstaw do wykluczenia w oparciu o art.25 ust..5 pkt 1:

1) **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 wykluczenia na podstawie art. 24 ust. 5 pkt. 1 ustawy;

dotyczy: odpisu z Krajowego Rejestru Sądowego (dla podmiotów wpisanych do KRS) lub odpisu z Centralnej Ewidencji Działalności Gospodarczej (dla podmiotów wpisanych do CEDIG) – wskazane rejestry są ogólnodostępnymi i bezpłatnymi bazami danych, zatem zamawiający pobierze samodzielnie informacje z tych baz.

6.2 **W celu potwierdzenia braku podstaw wykluczenia** wykonawcy z udziału w postępowaniu:

1) **informacji z Krajowego Rejestru Karnego** w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 Ustawy Pzp, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
2) **zaświadczenia właściwego naczelnika urzędu skarbowego** potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.
3) **zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych** lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.
4) **oświadczenia wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu** lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo - w przypadku wydania takiego wyroku lub decyzji - dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności,
5) **oświadczenia wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne.**
6) **oświadczenia wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych**, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 2016 r. poz. 716).

6.3 W celu potwierdzenia spełniania warunków udziału w postępowaniu:

1) **wykazu dostaw wykonanych,** a w przypadku świadczeń okresowych lub ciągłych również wykonywanych w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy-w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów- oświadczenie wykonawcy, w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

Z treści wykazu i dowodów potwierdzających wykonanie robót musi wynikać spełnianie warunku, o którym mowa w Rozdziale V.1.2) c).

7. W przypadku wykonawców składających wspólną ofertę, każdy z wykonawców musi złożyć dokument wymieniony w punkcie 6 ppkt.1). Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarciu umowy w sprawie zamówienia publicznego.

8. Wszyscy wykonawcy składający wspólną ofertę będą ponosić odpowiedzialność solidarną za wykonanie umowy.

9. Spółka cywilna jest kwalifikowana jako wykonawcy wspólnie ubiegający się o udzielenie zamówienia, dlatego jej wspólnicy zobowiązani są ustanowić pełnomocnika do reprezentowania w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo musi być załączone do oferty. Ponadto, każdy ze wspólników spółki cywilnej zobowiązany jest załączyć dokumenty wymienione w punkcie 6.2.

10. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub w jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić zamawiającemu, że realizując zamówienie, będzie realnie

dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

11. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w punkcie 6 ppkt. 1).

12. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa:

a) w pkt. 6.1 ppkt 1) - składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny dokument potwierdzający, że nie otwarto jego likwidacji ani nie ogłoszono upadłości,
- 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 pkt. a), zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo 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 miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby.

- dokumenty, o których mowa lit. a), powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

b) w pkt. 6.2 ppkt 1) - składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21. Dokumenty powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

c) w pkt. 6.2 ppkt 2) i 3) - składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi

odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

d) Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w pkt. 6.2 ppkt 1), składa dokument, w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 ustawy. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Dokument musi być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

   UWAGA: Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

   13. Oświadczenia, o których mowa w rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzieleniu zamówienia (Dz. U. z 2016r., poz. 1126 ze zm.) dotyczące wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art.22a ustawy oraz dotyczące podwykonawców muszą być złożone w oryginale, podpisane kwalifikowalnym podpisem elektronicznym. Dokumenty, o których mowa w rozporządzeniu, inne niż oświadczenia, o których mowa w zdaniu poprzednim, składać należy w oryginale lub kopii poświadczonej za zgodność w oryginałem w sposób zgodny z Rozporządzeniem Ministra Rozwoju z dnia 27 lipca 2016r. w sprawie rodzajów dokumentów jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016r. poz.1126 ze zm.

Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.

Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentów, o których mowa w rozporządzeniu, innych niż oświadczenia, wyłącznie wtedy, gdy złożona kopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jej prawdziwości.

14. Niedostarczenie któregokolwiek z wymaganych w specyfikacji oświadczeń lub dokumentów spowoduje wykluczenie wykonawcy lub odrzucenie oferty z zastrzeżeniem art. 26 ust. 1, 2, 3 i 3a ustawy - Prawo zamówień publicznych.

15. Jeżeli jest to niezbędna 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 oraz 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.

16. W przypadku wskazania przez Wykonawcę dostępności dokumentów w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych Zamawiający pobierze samodzielnie z tych baz danych wskazane przez Wykonawcę dokumenty. Wykonawca powinien w ofercie wskazać adres internetowy pod którym dostępne są te dokumenty. W przypadku samodzielnego pobrania przez zamawiającego z ogólnodostępnych i bezpłatnych baz danych wskazanych przez wykonawcę oświadczeń i dokumentów zamawiający będzie żądał od wykonawcy przedstawienia tłumaczenia na język polski ww. dokumentów.

ROZDZIAŁ VII. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

I. Informacje ogólne

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu miniPortalu https://miniportal.uzp.gov.pl/ , ePUAPu https://epuap.gov.pl/wps/portal oraz poczty elektronicznej - **Adres elektronicznej skrzynki podawczej ePUAP: /UJK/SkrytkaESP**

2. Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami: Pani Marcin Kmieciak e mail marcin.kmieciak@ujk.edu.pl tel. 41 349 7365 Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.
3. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP.
4. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty lub wniosku oraz do komunikacji wynosi 150 MB.
5. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
6. Identyfikator postępowania i klucz publiczny dla danego postępowania o udzielenie zamówienia dostępne są na *Liście wszystkich postępowań* na miniPortalu oraz stanowi załącznik do niniejszej SIWZ.

II. Złożenie oferty

1. Wykonawca składa ofertę za pośrednictwem ***Formularza do złożenia, zmiany, wycofania oferty lub wniosku*** dostępnego na ePUAP i udostępnionego również na miniPortalu. Klucz publiczny niezbędny do zaszyfrowania oferty przez Wykonawcę jest dostępny dla wykonawców na miniPortalu. W formularzu oferty Wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.
2. Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w formacie danych doc. docx i podpisana kwalifikowanym podpisem elektronicznym. Sposób złożenia oferty, w tym zaszyfrowania oferty opisany został w Regulaminie korzystania z miniPortal. Ofertę należy złożyć w oryginale. Zamawiający nie dopuszcza możliwości złożenia skanu oferty opatrzonej kwalifikowanym podpisem elektronicznym.

3. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP).
4. Do oferty/wniosku należy dołączyć Jednolity Europejski Dokument Zamówienia w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
5. Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionych również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu
6. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
7. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim**.**

III. Sposób komunikowania się Zamawiającego z Wykonawcami (nie dotyczy składania ofert)

1. W postępowaniu o udzielenie zamówienia komunikacja pomiędzy Zamawiającym a Wykonawcami w szczególności składanie oświadczeń, wniosków (innych niż wskazanych w pkt II), zawiadomień oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem ***dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji).*** We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP, TED lub ID postępowania).
2. Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej, email marcin.kmieciak@ujk.edu.pl
3. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem *Formularza do komunikacji* jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na wskazany w

pkt 2 adres email. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. *w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych* oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. *w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.*

ROZDZIAŁ VIII. WYMAGANIA DOTYCZĄCE WADIUM

1. Warunkiem udziału w postępowaniu jest wniesienie wadium w kwocie:

1300 zł (słownie złotych: jeden tysiąc trzysta złotych 00/100).

Wadium należy wnieść przed upływem terminu składania ofert.

2. Wadium może być wnoszone w jednej lub kilku następujących formach:

a) pieniądzu,

b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym;

c) gwarancjach bankowych;

d) gwarancjach ubezpieczeniowych;

e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2014 r. poz. 1804 oraz z 2015 r. poz. 978 i 1240).

3. Wadium w formie pieniądza należy wnieść przelewem na numer konta na konto Uniwersytetu Jana Kochanowskiego w Kielcach Bank Millenium S.A. Nr 15 1160 2202 0000 0003 3977 3201.

4. Na dowodzie przelewu należy wpisać: „Wadium – oznaczenie sprawy DP.2301.8.2019”

5. Potwierdzoną za zgodność z oryginałem kopię dowodu wpłaty można dołączyć do oferty.

6. Wadium, jako jeden z dokumentów niezbędnych do złożenia skutecznej i ważnej oferty powinno być wniesione w postaci elektronicznej. Wadium w formie innej niż pieniądz wykonawca wnosi w formie elektronicznej poprzez wczytanie na miniPortalu oryginału dokumentu wadialnego, tj. opatrzonego kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia.

7. Oferta niezabezpieczona jedną z form wadium zostanie odrzucona zgodnie z art. 89 ust. 1 pkt. 7a) ustawy PZP.

8. Zwrot wadium nastąpi zgodnie z art. 46 ust. 1, ust. 1a, ust. 2 ustawy PZP.

ROZDZIAŁ IX. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca będzie związany złożoną ofertą przez **60 dni**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Wykonawca samodzielnie lub na wniosek zamawiającego może przedłużyć termin związania ofertą, z tym, że zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

ROZDZIAŁ X. OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej. Oferta musi być sporządzona czytelnie, w języku polskim, oraz podpisana kwalifikowalnym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w Ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579) przez osobę uprawnioną /osoby uprawnione do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty. W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) wykonawcy, należy do oferty dołączyć stosowane pełnomocnictwo.

2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.

3. Jeżeli oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia zostanie wybrana, Zamawiający będzie żądał przed zawarciem umowy w sprawie zamówienia publicznego przedłożenia umowy regulującej współpracę tych wykonawców.

4. Wykonawcy występujący wspólnie ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zamówienia.

5. Dokumenty sporządzone w języku obcym muszą zostać złożone wraz z tłumaczeniem na język polski, poświadczone przez wykonawcę.

6. Każdy wykonawca może złożyć tylko jedną ofertę, która musi obejmować całość przedmiotu zamówienia.(części, której dotyczy składana oferta)

7. Treść złożonej oferty musi odpowiadać treści niniejszej SIWZ.

8. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

9. Zaleca się, aby każda zapisana strona oferty była ponumerowana kolejnymi numerami.

10. Zamawiający informuje, iż zgodnie z art. 8 w związku z art. 96 ust. 3 ustawy PZP oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa, jeśli wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępnione i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa, oraz z wyjątkiem informacji podlegających ochronie danych osobowych (RODO).

11. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnym pliku oznaczonym jako: „tajemnica przedsiębiorstwa", Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń. W przypadku zastrzeżenia określonych informacji jako tajemnicy przedsiębiorstwa należy w ofercie wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa (art.8 ust.3 PZP)
12. Zamawiający informuje, że w przypadku kiedy wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnice 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.
13. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że zamawiający otrzyma elektroniczne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone wg takich samych zasad, jak składana oferta, tj. w formie elektronicznej, w sposób wskazany w załączniku nr 7 do SIWZ, plik musi być oznaczony jako „ZMIANA". Pliki oznaczone jako „ZMIANA" zostaną otwarte przy otwieraniu oferty wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.

14. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie elektronicznego powiadomienia, według tych samych zasad jak

wprowadzenie zmian i poprawek z oznaczeniem pliku jako „WYCOFANIE”. Pliki oznaczone w ten sposób będą otwierane w pierwszej kolejności.

15. Oferta, której treść nie będzie odpowiadać treści niniejszej SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt. 3 ustawy PZP zostanie odrzucona (art. 89 ust. 1 pkt. 2 ustawy PZP). Wszelkie niejasności i obiekcje dotyczące treści zapisów w niniejszej SIWZ należy zatem wyjaśnić z zamawiającym przed terminem składania ofert w trybie przewidzianym w niniejszej SIWZ. Przepisy ustawy PZP nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.

ROZDZIAŁ XI. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Ofertę, wraz z wymaganymi dokumentami, należy złożyć zgodnie z opisem zawartym w Rozdziale VII SIWZ. Oferta i dokumenty muszą być podpisane bezpiecznym podpisem elektronicznym wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. – o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r. poz. 1579).
2. O terminie złożenia oferty decyduje czas pełnego przeprocesowania transakcji na miniPortalu.
3. Po upływie terminu, o którym mowa powyżej, złożenie oferty jest możliwe, jednak taka oferta, w terminach przewidzianych w art. 84 ust. 2 Ustawy Prawo zamówień publicznych, zostanie zwrócona Wykonawcy. Uwaga! O terminie złożenia oferty decyduje czas ostatecznego wysłania oferty a nie czas rozpoczęcia jej wprowadzenia.
4. Ofertę należy złożyć za pośrednictwem Platformy Przetargowej do dnia **01.04.2019** r. do godziny **10:00**.
5. Publiczne otwarcie ofert nastąpi w dniu **01.04.2019** r. o godzinie **11:00,** w siedzibie zamawiającego:

   Uniwersytet Jana Kochanowskiego w Kielcach

   25 – 369 Kielce, ul. Żeromskiego 5

   Dział Zamówień Publicznych

6. Otwarcie ofert następuje poprzez użycie aplikacji do szyfrowania ofert dostępnej na miniPortalu i dokonywane jest poprzez odszyfrowanie i otwarcie ofert za pomocą klucza prywatnego.

7. Otwarcie ofert jest jawne, Wykonawcy mogą uczestniczyć w sesji otwarcia ofert.
8. Podczas otwarcia ofert zamawiający odczyta informacje, o których mowa w art. 86 ust. 4 ustawy PZP.
9. Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie internetowej informację z otwarcia ofert.

ROZDZIAŁ XII. OPIS SPOSOBU OBLICZENIA CENY

1. Rozliczenia pomiędzy wykonawcą, a zamawiającym będą dokonywane wyłącznie w złotych polskich.
2. W ofercie cena ryczałtowa brutto musi być podana w złotych polskich cyfrowo i słownie, w zaokrągleniu do drugiego miejsca po przecinku.
3. Jeżeli w postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. W takim przypadku Wykonawca, składając ofertę, jest zobligowany poinformować zamawiającego, że wybór jego oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru / usługi, których dostawa / świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku. Niezłożenie przez Wykonawcę informacji będzie oznaczało, że taki obowiązek nie powstaje.
4. Prawidłowe ustalenie podatku VAT należy do obowiązków Wykonawcy.
5. Oferta musi zawierać ostateczną, sumaryczną cenę obejmującą wszystkie koszty z uwzględnieniem wszystkich opłat i podatków (także podatku od towarów i usług) oraz ewentualnych upustów i rabatów. Przy dokonywaniu wyceny przedmiotu zamówienia należy uwzględnić wszystkie dane z analizy opisu przedmiotu zamówienia. Koszty związane z opracowaniem oferty ponosi Wykonawca).
6. W związku z powyższym cena oferty winna zawierać wszelkie koszty niezbędne do zrealizowania zamówienia z uwzględnieniem ryzyka Wykonawcy, w tym także opłaty związane z dostawą, w tym transportu wyposażenia do miejsc wskazanych przez zamawiającego (na terenie miasta Kielce), wniesienia do wskazanych pomieszczeń, instalację, uruchomienie i przeszkolenie pracowników zamawiającego z zakresu obsługi dostarczonego wyposażenia.

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

1. Zamawiający za najkorzystniejszą uzna ofertę niepodlegającą odrzuceniu, która uzyska największą liczbę punktów obliczona w oparciu o podane kryteria oceny ofert.
2. Zamawiający dokona oceny ofert według następujących kryteriów i ich wag:

Lp.	Kryterium	Waga kryterium	Maksymalna ilość punktów jakie może otrzymać oferta za kryterium
1	cena brutto	100%	100

3. W trakcie oceny ofert kolejno ocenianym ofertom, zostaną przyznane punkty wg poniższego wzoru:

1) Sposób oceny ofert dla kryterium nr 1 - cena brutto (1):

najniższa oferowana cena brutto

---------- x 100 pkt

cena brutto badanej oferty

2) Punktacja przyznawana ofertom będzie liczona z dokładnością do dwóch miejsc po przecinku. Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.

4. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie Prawo zamówień publicznych i Specyfikacji Istotnych Warunków Zamówienia oraz zostanie oceniona jako najkorzystniejsza w oparciu o podane w rozdz. XIII kryterium oceny ofert dla przedmiotu zamówienia.
5. Zamawiający poinformuje niezwłocznie wszystkich wykonawców o wyborze najkorzystniejszej oferty, podając informacje, o których mowa w art. 92 ust. 1 ustawy PZP.
6. Zamawiający udostępnia informacje, o których mowa w art. 92 ust. 1 pkt. ustawy PZP, na stronie internetowej www.ujk.edu.pl

ROZDZIAŁ XIV. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, ZAWARCIE UMOWY

1. W przypadku wyboru oferty złożonej przez wykonawców wspólnie ubiegających się o udzielenie zamówienia zamawiający będzie żądał przed zawarciem umowy przedstawienia umowy regulującej współpracę tych wykonawców. Umowa taka winna

określać strony umowy, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdemu z nich, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania konsorcjum (obejmującego okres realizacji przedmiotu zamówienia), wykluczenie możliwości wypowiedzenia umowy konsorcjum przez któregokolwiek z jego członków do czasu wykonania zamówienia.

2. Zamawiający **nie będzie żądał** od Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, wniesienia zabezpieczenia należytego wykonania umowy.
3. Zamawiający zawrze umowę w sprawie zamówienia publicznego w terminach określonych w art. 94 ust. 1 lub ust. 2 ustawy Pzp.
4. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, przed podpisaniem umowy zobowiązany jest do złożenia informacji o osobach umocowanych do zawarcia umowy i jeżeli taka konieczność zaistnieje - złożenia ich pełnomocnictw w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza lub osobę/osoby udzielające pełnomocnictwa.
5. Wybranemu Wykonawcy Zamawiający wskaże termin i miejsce podpisania umowy.

ROZDZIAŁ XV. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie będzie żądał od Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XVI. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ PROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, OGÓLNE WARUNKI UMOWY.

1. Zawarcie umowy nastąpi według wzoru Zamawiającego – stanowiącego załącznik nr 3 SIWZ.
2. Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru wykonawcy, w szczególności w poniższych przypadkach i w okolicznościach określonych art.144 ust.1 Pzp.

1) Terminu wykonania umowy, w przypadku zaistnienia w przypadku zaistnienia okoliczności, na które Strony umowy nie miały wpływu (w tym również w przypadku klęski żywiołowej, zjawisk atmosferycznych, siły wyższej, sytuacji, których nie dało się przewidzieć, które mają wpływ na termin realizacji i są niezależne od stron umowy). Zmiana terminu realizacji zamówienia może nastąpić wyłącznie na uzasadniony/zaakceptowany przez zamawiającego wniosek wykonawcy zawierający uzasadnienie zmiany terminu; w szczególności zmiana terminu wykonania przedmiotu

umowy może ulec zmianie przypadku wystąpienia zdarzenia losowego mającego charakter siły wyższej uniemożliwiającej wykonanie przedmiotu umowy zgodnie z jej postanowieniami.

W przypadku wystąpienia sytuacji skutkujących koniecznością zmiany umowy z przyczyn, o których mowa wyżej, wykonawca zobowiązany jest do niezwłocznego poinformowania, o tym fakcie zamawiającego i wystąpienia z wnioskiem o dokonanie wskazanej zmiany. Zmiana umowy powinna nastąpić w formie pisemnego aneksu sporządzonego przez zamawiającego i podpisanego przez strony umowy, pod rygorem nieważności takiego oświadczenia oraz powinna zawierać uzasadnienie faktyczne i prawne.

2) Zmiana podwykonawców, w tym podwykonawców na zasobach, których wykonawca opierał się wykazując spełnianie warunków udziału w postępowaniu, pod warunkiem, że nowy podwykonawca wykaże spełnianie warunków w zakresie nie mniejszym niż wymagane w SIWZ (taka zmiana nie wymaga aneksu).
3) Wprowadzenie przez wykonawcę podwykonawcy pomimo wykazania w ofercie wykonania przedmiotu umowy siłami własnymi, pod warunkiem uzgodnienia tego podwykonawcy z zamawiającym i treści umowy z nim zawartej przez wykonawcę (taka zmiana nie wymaga aneksu). Jeżeli powierzenie podwykonawcy wykonania części zamówienia nastąpi w trakcie jego realizacji, wykonawca przedstawi zamawiającemu oświadczenie, o którym mowa w art. 25a ust. 1 Pzp i dokument potwierdzający brak podstaw wykluczenia wobec tego podwykonawcy.

Jeżeli zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą podstawy wykluczenia, wykonawca obowiązany jest zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia podwykonawcy. (art.36ba Pzp).

4) zmiana oprogramowania, jeżeli zaproponowane w ofercie zostanie wycofane z produkcji lub zastąpiony nowszą wersją – pod warunkiem, że nie będzie gorsze niż te wskazane w SIWZ oraz gwarantować będzie zachowanie parametrów i funkcjonalności opisanych w SIWZ Wykonawca w tym przypadku musi wykazać, że oferowany przez niego produkt spełnia, wymagania określone przez Zamawiającego oraz uzyskać zgodę zamawiającego na taką zmianę. Taka zmiana nie może skutkować zwiększeniem ceny za oprogramowanie Taka zmiana nie wymaga aneksu do umowy.

W przypadku wystąpienia sytuacji skutkujących koniecznością zmiany umowy z przyczyn, o których mowa wyżej, Wykonawca zobowiązany jest do niezwłocznego poinformowania, o tym fakcie zamawiającego i wystąpienia z wnioskiem o dokonanie wskazanej zmiany.

Zmiana umowy powinna nastąpić w formie pisemnego aneksu sporządzonego przez zamawiającego i podpisanego przez strony umowy, pod rygorem nieważności takiego oświadczenia oraz powinna zawierać uzasadnienie faktyczne i prawne.

Zmiana do umowy w sprawie zamówienia publicznego bez zachowania formy pisemnej jest dotknięta sankcją nieważności, a więc nie wywołuje skutków prawnych.

ROZDZIAŁ XVII. INFORMACJA DOTYCZĄCA WALUT OBCYCH W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich.

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

1. Uczestnikom niniejszego postępowania przysługują środki odwoławcze opisane w Dziale VI ustawy PZP.
2. 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.
3. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.
4. 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.
5. Odwołanie wnosi się w terminie 10 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 Pzp, albo w terminie 15 dni - jeżeli zostały przesłane w inny sposób.
6. Odwołanie wobec treści ogłoszenia o zamówieniu i postanowień SIWZ wnosi się w terminie 10 dni od dnia wysłania ogłoszenia do publikacji w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia specyfikacji istotnych warunków zamówienia na stronie internetowej.
7. Odwołanie wobec czynności innych niż określone w pkt 5 i 6 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

8. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.

9. Wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje, i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje. Zgłoszenie przystąpienia doręcza się Prezesowi Izby w postaci papierowej albo elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, a jego kopię przesyła się zamawiającemu oraz wykonawcy wnoszącemu odwołanie.

10. Wykonawcy, którzy przystąpili do postępowania odwoławczego, stają się uczestnikami postępowania odwoławczego, jeżeli mają interes w tym, aby odwołanie zostało rozstrzygnięte na korzyść jednej ze stron.

11. Zamawiający lub odwołujący może zgłosić opozycję przeciw przystąpieniu innego wykonawcy nie później niż do czasu otwarcia rozprawy.

12. Jeżeli koniec terminu do wykonania czynności przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następnego po dniu lub dniach wolnych od pracy.

13. Dokładne informacje dotyczące środków ochrony prawnej zawarte są w ustawie z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, w Dziale VI – Środki ochrony prawnej.

UWAGA:

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:

administratorem Pani/Pana danych osobowych jest Uniwersytet Jana Kochanowskiego w Kielcach, 25-369 Kielce ul. Żeromskiego 5, tel. 41 349 72 00; fax: 41 344 5615;

Uniwersytet Jana Kochanowskiego w Kielcach wyznaczył inspektora ochrony danych osobowych, z którym można się skontaktować pod numerem telefonu: 41 349 73 45 bądź adresem e-mail: iod@ujk.edu.pl

Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. :„Dostawa specjalistycznego sprzętu dla Wydziału Lekarskiego i Nauk o Zdrowiu UJK w Kielcach" nr DP.2301. 2. 2019 prowadzonym w trybie przetargu nieograniczonego;

odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp";

Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

posiada Pani/Pan:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowy;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

Integralną część niniejszej SIWZ stanowią:

Załącznik nr 1- Opis przedmiotu zamówienia.

Załącznik nr 2- Formularz ofertowy

Załącznik nr 3 - Wzór umowy

Załącznik nr 4 - JEDZ

Załącznik nr 5 - Wykaz dostaw

Załącznik nr 6- Oświadczenie dotyczące grupy kapitałowej

Komisja akceptuje treść specyfikacji:

1. Andrzej Ososiński…….
2. Olga Kalińska……
3. Marcin Borej……..
4. Beata Szwajkiwska……
5. Marcin Kmieciak ……..

---

* 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.

Załącznik nr 2 do SIWZ

Dane Wykonawcy

Nazwa Wykonawcy:

……

Siedziba:

……

Nr KRS: …….

Adres do korespondencji: ……..……

Adres poczty elektronicznej …….

Adres elektronicznej skrzynki podawczej ePUAP: ……

Strona internetowa ……..……..……..

Numer telefonu ……..

Numer faksu..……..

OFERTA

Uniwersytet Jana Kochanowskiego w Kielcach

ul. Żeromskiego 5, 25-369 Kielce

1. W odpowiedzi na ogłoszenie przez Uniwersytet Jana Kochanowskiego w Kielcach przetargu nieograniczonego, którego przedmiotem jest „***Dostawa oprogramowania antywirusowego wraz z konsolą do zarządzania.”*** (postępowanie nr DP.2301.8.2019), przedkładamy niniejszą ofertę oświadczając, że akceptujemy w całości wszystkie warunki zawarte w Specyfikacji Istotnych Warunków Zamówienia (SIWZ).

2. Oferujemy wykonanie przedmiotu zamówienia w zakresie objętym specyfikacją istotnych warunków zamówienia i załącznikami do SIWZ **za cenę brutto** (łącznie z podatkiem VAT): ……zł (słownie złotych: ……);

   Na powyższą cenę składają się :

Lp.	NAZWA	ILOŚĆ	Wartość brutto
1			

3. Na dostarczone oprogramowanie udzielimy gwarancji 36 miesięcy

4. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
5. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia i nie wnosimy do nich żadnych zastrzeżeń. Zdobyliśmy również konieczne informacje potrzebne do właściwej wyceny oraz właściwego wykonania przedmiotu zamówienia.
6. Oświadczamy, że zawarty w Specyfikacji Istotnych Warunków Zamówienia wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty, do zawarcia umowy na wymienionych w nim warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.
7. Termin płatności – 30 dni od daty otrzymania przez zamawiającego prawidłowo wystawionej faktury wraz z końcowym protokołem odbioru.
8. Termin dostawy : ……

9. Przedmiot zamówienia zamierzamy wykonać sami bez udziału podwykonawców/ z udziałem podwykonawców*

* niewłaściwe skreślić

10. Podwykonawcom zamierzamy powierzyć następującą cześć zamówienia:

1) ……, nazwa firmy podwykonawcy……

2) ……, nazwa firmy podwykonawcy……

11. Oświadczam, że jestem / nie jestem mikroprzedsiębiorstwem, małym lub średnim przedsiębiorstwem zgodnie z definicją zawartą w zaleceniu Komisji z dn. 6 maja 2003 r. dotyczącym definicji przedsiębiorstw mikro, małych i średnich (Dz. Urz. UE nr 2003/361/WE). W przypadku zaznaczenia powyżej odpowiedzi twierdzącej, należy poniżej zaznaczyć krzyżykiem odpowiedni kwadrat:

□ mikroprzedsiębiorstwo □ małe przedsiębiorstwo □ średnie przedsiębiorstwo

12. INFORMUJEMY, że:

wybór oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego**) w odniesieniu do następujących towarów/ usług (w zależności od przedmiotu zamówienia): _____. Wartość towaru/usług (w zależności od przedmiotu zamówienia) powodująca obowiązek podatkowy u Zamawiającego to _____ zł netto.

**) Dotyczy Wykonawców, których oferty będą generować obowiązek doliczania wartości podatku VAT do przedstawionej w niej ceny, tj. w przypadku:

wewnątrzwspólnotowego nabycia towarów,

mechanizmu odwróconego obciążenia, o którym mowa w art. 17 ust. 1 pkt 7 ustawy o podatku od towarów i usług,

importu usług lub importu towarów, z którymi wiąże się obowiązek doliczenia przez zamawiającego przy porównywaniu cen ofertowych podatku VAT.

informacje i dokumenty zawarte na stronach nr od ___ do ____ stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i zastrzegamy, że nie mogą być udostępniane. Uzasadnienie zastrzeżenia ww. dokumentów i informacji jako tajemnicy przedsiębiorstwa został zawarte na stronach nr od ___ do ___.

13. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.*

..... dnia ..... 2019r.

(miejscowość)

.....

Czytelne podpisy osób uprawnionych
do składania oświadczeń woli w imieniu
Wykonawcy

1) rozporządzenie 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).

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

Załącznik nr 3 PROJEKT UMOWY

UMOWA NR DP……..2019

zawarta w dniu …….2019 roku w Kielcach pomiędzy:
Uniwersytetem Jana Kochanowskiego w Kielcach z siedzibą w Kielcach przy ul. Żeromskiego 5, zwanym w dalszej części „Zamawiającym”, reprezentowanym przez:
Dr Aleksandrę Pisarską – Kanclerza UJK
a

zwanym w dalszej części „Wykonawcą”, reprezentowanym przez:

W rezultacie dokonania wyboru oferty Wykonawcy w drodze postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, na podstawie ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych ((Dz. U. z 2018 r., poz. 1986 z późn. zm.), o następującej treści:

§ 1.

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu oprogramowanie wraz z nie wyłącznymi licencjami na okres **3 lat** :

   a) licencje oprogramowania antywirusowego na **2200** stanowisk komputerowych (serwerów i urządzeń mobilnych) wraz z niewyłącznymi licencjami na okres trzech lat, gdzie co najmniej 25 % z tej puli można wykorzystać w ochronie systemów serwerowych

   zgodnie ze Specyfikacją Istotnych Warunków Zamówienia i złożoną ofertą, które stanowią integralną część niniejszej umowy.
2. Cena sprzedaży uwzględnia koszty: transportu oprogramowania do siedziby użytkownika.

3. Wykonawca zobowiązany jest do przeprowadzenia procedury instalacji, konfiguracji i uruchomienia oprogramowania, przeszkolenia pracowników,

4. Wykonawca zobowiązany jest do przeprowadzenia wdrożenia wraz z uruchomieniem oraz szkoleniem z administrowania systemem dla co najmniej 15 wskazanych pracowników Zamawiającego w siedzibie Zamawiającego. Szkolenie trwające nie krócej jak 8 godzin roboczych, Instalacja systemu antywirusowego w siedzibie Zamawiającego, asysta przy migracji do nowego systemu antywirusowego – co najmniej 8 godzin. Wsparcie techniczne : bezpłatna pomoc techniczna w okresie ważności licencji świadczona przez przeszkolonego inżyniera w języku polskim w dni robocze w godz. 8 -16. Wykonawca zapewni bezpłatne aktualizacje baz sygnatur wirusów oraz zakupionego oprogramowania w okresie

ważności licencji. Wykonawca jest zobowiązany do dostarczania zaktualizowanych najnowszych wersji oprogramowania antywirusowego w ramach ustalonego wynagrodzenia w okresie trwania umowy.

5. Cena sprzedaży uwzględnia również koszty przekazania licencji na korzystanie z oprogramowania zgodnie ze Specyfikacją Istotnych Warunków Zamówienia i złożoną ofertą, które stanowią integralną część niniejszej umowy.

6. Dostawa (instalacja, konfiguracja i uruchomienie i przeszkolenie pracowników a także inne czynności objęte zakresem umowy) oprogramowania nastąpi w terminie do **…….2019 r.** Licencje będą ważne trzy lata od dnia zakończenia czynności dostawy.

7. Zmiana terminu, o którym mowa w ust. 3 niniejszego paragrafu może nastąpić wyłącznie w przypadku wystąpienia okoliczności niezawinionych przez Wykonawcę, których mimo dołożenia należytej staranności nie można było przewidzieć, w szczególności będących następstwem działania siły wyższej.

8. Przez siłę wyższą Strony rozumieją nadzwyczajne zdarzenie zewnętrzne, niezależne od woli Stron, którego Strona nie mogła przewidzieć oraz któremu nie mogła zapobiec, a które faktycznie bezpośrednio uniemożliwia lub zasadniczo utrudnia realizację przedmiotu umowy, w szczególności wojnę, przewrót, zamieszki, rebelia, strajk w branżach mających zasadniczy wpływ na terminową realizację umowy, decyzje odpowiednich władz mające wpływ na wykonanie umowy.

9. Zmiana terminu realizacji umowy może nastąpić wyłącznie za zgodą Zamawiającego na pisemny wniosek Wykonawcy, zawierający uzasadnienie zmiany terminu.

§ 2.

1. Wynagrodzenie z tytułu wykonania umowy obejmuje wszystkie koszty związane z jej realizacją, łącznie z transportem, (instalacja oprogramowania na wskazanych przez zamawiającego urządzeniach) oraz koszty licencji na określonych w umowie polach eksploatacji, w tym także sublicencji i uaktualnień

2. Zamawiający zobowiązuje się zapłacić za wykonanie umowy cenę brutto **…….. zł** (słownie złotych: ……*/100*) w tym podatek VAT zgodny z obowiązującymi przepisami.

3. Odbioru przedmiotu umowy dokona komisja składająca się z użytkownika oprogramowania, osoby materialnie odpowiedzialnej i przedstawiciela Wykonawcy, w ciągu 2 dni licząc od dnia zgłoszenia oprogramowania do

odbioru. Podstawą do wystawienia faktury będzie podpisany protokół odbioru sprzętu komputerowego i prac określonych w § 1 ust. 4. stanowiący załącznik do umowy.

§ 3.

1. Osoba wyznaczona do kontaktów po stronie Wykonawcy: …….
2. W przypadku zmiany osoby odpowiedzialnej za kontakt z Zamawiającym, Wykonawca niezwłocznie zawiadomi na piśmie o tym fakcie Zamawiającego.

§ 4.

1. Wykonawca udziela 36 miesięcznej gwarancji, licząc od dnia podpisania bezusterkowego protokołu odbioru, na oprogramowanie na warunkach określonych w SIWZ oraz na poniższych warunkach:

a) Oprogramowanie licencjonowane przez Wykonawcę będzie działało zgodnie ze specyfikacją wymagań zamieszczonych w SIWZ

b) Gwarancja na oprogramowanie osób trzecich (oprogramowanie zewnętrzne) będzie świadczona zgodnie z warunkami zapewnianymi przez producenta tego oprogramowania

2. Wykonawca udziela 36 miesięcznej gwarancji na nośniki na których znajduje się oprogramowanie
3. W ramach gwarancji Wykonawca zobowiązany jest do bezpłatnego usunięcia występujących awarii/wad/usterek lub błędów w pracy oprogramowania
4. W okresie gwarancji Wykonawca zobowiązany będzie do nieodpłatnego przekazania Zamawiającemu aktualnych wersji oprogramowania.

§ 5.

1. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady uniemożliwiające prawidłowe zainstalowanie, uruchomienie lub korzystanie z oprogramowania.
2. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne przedmiotu umowy, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych za znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzaniem towarów do obrotu na terytorium Rzeczypospolitej Polskiej.
3. Wykonawca zobowiązany jest do pokrycia Zamawiającemu ewentualnych roszczeń osób trzecich wynikających z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki

towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzaniem towarów do obrotu na terytorium Rzeczypospolitej Polskiej.

4. Wykonawca oświadcza, że autorzy oprogramowania ani osoby trzecie nie będą zgłaszać względem Zamawiającego żadnych roszczeń, w tym z tytułu swoich autorskich praw osobistych, ani roszczeń z tytułu autorskich praw majątkowych w stosunku do oprogramowania lub poszczególnych jego części będących przedmiotem niniejszej umowy. W przypadku wystąpienia względem Zamawiającego przez osoby trzecie z roszczeniami o których mowa w zdaniu poprzednim Wykonawca zobowiązany jest do pokrycia Zamawiającemu wszelkich kosztów, w tym kosztów postępowania sądowego związanych z roszczeniami osób trzecich.
5. Na mocy niniejszej umowy Wykonawca udziela Zamawiającemu niewyłącznej bezterminowej licencji na korzystanie na terytorium Rzeczypospolitej Polskiej z oprogramowania na ilości stanowisk zgodnych ze SIWZ na następujących polach eksploatacji:

    a) wprowadzanie oprogramowania do pamięci komputerów (serwerów i urządzeń mobilnych) Zamawiającego,

    b) usuwania z pamięci komputerów (serwerów i urządzeń mobilnych)

    c) stosowanie oprogramowania zgodnie z jego przeznaczeniem na stanowiskach komputerowych (serwerów , urządzeń mobilnych) pozostających pod kontrolą Zamawiającego,

    d) korzystanie z dokumentacji dostarczonej przez Wykonawcę,

    e) tłumaczenie, przystosowywanie, zmiany układu lub jakiekolwiek inne zmian w oprogramowaniu, w zakresie dozwolonym przez przepisy prawa autorskiego,

    f) modyfikowania i rozbudowy oprogramowania lub łączenie go z innym programem lub programami na zasadach określonych przepisami prawa autorskiego,

    g) wykorzystanie oprogramowania podczas pokazów lub prezentacji publicznych,

    h) trwałe lub czasowe zwielokrotnianie oprogramowania w całości lub części jakimikolwiek środkami lub w jakiejkolwiek formie w zakresie niezbędnym dla realizacji uprawnień określonych w pkt.1-5 powyżej.

§ 6.

1. Zapłata za dostarczony przedmiot umowy określony w § 1 nastąpi na podstawie prawidłowej faktury VAT wystawionej po podpisaniu bezusterkowego protokołu odbioru, stanowiącym załącznik do niniejszej umowy.
2. Protokół odbioru musi być zatwierdzony przez strony.
3. Dane płatnika: Uniwersytet Jana Kochanowskiego w Kielcach, 25 – 369 Kielce, ul. Żeromskiego 5, NIP 657-02-34-850.
4. Zamawiający zobowiązuje się uregulować fakturę VAT Wykonawcy w terminie 30 dni licząc od daty jej doręczenia do Zamawiającego – przelewem na numer konta bankowego Wykonawcy……
   Za datę zapłaty strony przyjmują datę obciążenia rachunku bankowego Zamawiającego.
5. Wykonawca oświadcza, że jest podatnikiem VAT i posiada NIP: …….

§ 7.

1. W przypadku niewykonania lub nienależytego wykonania umowy Wykonawca zobowiązuje się zapłacić kary umowne w wysokości:
   1) 0,2% ceny umowy brutto za każdy rozpoczęty dzień opóźnienia w wykonaniu umowy,
   2) 0,2% ceny umowy brutto za każdy dzień opóźnienia w usunięciu występujących wad w okresie gwarancji lub rękojmi,
   3) 15% ceny umowy brutto jeżeli dojdzie do odstąpienia od umowy z przyczyn zależnych od Wykonawcy.
2. Strony zastrzegają sobie możliwość dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych Kodeksu cywilnego.
3. W przypadku niewykonania lub nienależytego wykonania umowy Zamawiający zobowiązuje się zapłacić kary umowne w wysokości:
   1) 0,2% wartości umowy brutto za każdy rozpoczęty dzień zwłoki w odbiorze przedmiotu umowy,
   2) 15% wartości umowy brutto jeżeli dojdzie do odstąpienia od umowy z przyczyn zależnych od Zamawiającego. Niniejszy zapis nie ma zastosowania w przypadku odstąpienia od umowy na podstawie art. 145 ustawy Prawo zamówień publicznych.
4. Zamawiający ma prawo potrącenia kar umownych z należnego Wykonawcy Wynagrodzenia

§ 8.

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. Zakazuje się istotnych zmian postanowień zawartej umowy w stosunku do treści oferty na podstawie, której dokonano wyboru Wykonawcy, chyba że Zamawiający przewidział możliwość dokonania takiej zmiany w ogłoszeniu o zamówieniu lub w Specyfikacji Istotnych Warunków Zamówienia oraz określił warunki takiej zmiany.
3. Oprócz przypadków wymienionych w przepisach Kodeksu cywilnego, Zamawiający może odstąpić od umowy w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili jej zawarcia. Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.

§ 9.

Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji uzyskanych w trakcie realizacji umowy z wyjątkiem informacji, których ujawnienia wymagają przepisy prawa powszechnie obowiązującego, ale tylko w niezbędnym do tego obowiązku zakresie.

§ 10.

1. W sprawach nieuregulowanych umową będą miały zastosowanie przepisy ustawy Prawo zamówień publicznych i Kodeksu cywilnego.
2. Bez uprzedniej pisemnej zgody Zamawiającego nie jest dopuszczalny przelew wierzytelności przysługującej Wykonawcy z tytułu niniejszej umowy.
3. Wszelkie załączniki do umowy stanowią integralną jej część.

§ 11.

Spory wynikłe na tle realizacji umowy podlegają rozpatrzeniu według prawa polskiego przez właściwy rzeczowo sąd w Kielcach.

§ 12.

Adresem Wykonawcy do doręczeń wszelkiej korespondencji związanej z niniejszą umową jest adres wskazany powyżej w umowie. O każdej jego zmianie Wykonawca jest zobowiązany niezwłocznie powiadomić Zamawiającego. W przypadku zaniechania tego obowiązku, korespondencja wysłana do Wykonawcy na ostatni jego adres znany Zamawiającemu, uważana jest za skutecznie doręczoną.

§ 13.

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa dla Zamawiającego i jeden dla Wykonawcy.

WYKONAWCA ZAMAWIAJĄCY

PROTOKÓŁ ODBIORU z dnia ……

Dostawca: ……
……
……

Odbiorca: Uniwersytet Jana Kochanowskiego w Kielcach
ul. Żeromskiego 5, 25-369 Kielce

Miejsce odbioru: ……
……
……

Data odbioru: …….

Dostarczono:

Nazwa	Producent	Nr wersji	Ilość

Strony oświadczają, że dostarczone oprogramowanie jest zgodne/nie zgodne* ze specyfikacją, a dostawa została zrealizowana zgodnie/nie zgodnie* z zapisami umowy nr DP/2301….2019 z dnia ……

Strona odbierająca potwierdza, że wyżej wymienione oprogramowanie zostało odebrane bez zastrzeżeń jako w pełni sprawne przez uprawnionych pracowników.*

Strona odbierająca potwierdza że Wykonawca prawidłowo przeprowadził procedurę instalacji, konfiguracji i uruchomienia oprogramowania, oraz przeszkolenia pracowników

Strona odbierająca stwierdza, że nie dokonała odbioru z przyczyn określonych w uwagach do protokołu.*

Protokół spisano w dwóch jednobrzmiących egzemplarzach.

Strona przekazująca: Strona odbierająca:

…… ……..
(Czytelny podpis i pieczęć) (Czytelny podpis i pieczęć)

Osoba materialnie odpowiedzialna

……
(Czytelny podpis i pieczęć)

UWAGI

……

……

niepotrzebne skreśl

Kielce, dnia …… WZÓR

PROTOKÓŁ ODBIORU z dnia ……

Dostawca: ……

……

Odbiorca: Uniwersytet Jana Kochanowskiego w Kielcach

ul. Żeromskiego 5, 25-369 Kielce

Miejsce odbioru: ……

Data odbioru: ……

Dostarczono:

Nazwa	Producent	Nr wersji	Ilość

Strony oświadczają, że dostarczony sprzęt jest zgodny/nie zgodny* ze specyfikacją, a dostawa została zrealizowana zgodnie/nie zgodnie* z zapisami umowy nr DP/2301/…/19, z dnia ……

Strona odbierająca potwierdza, że wyżej wymieniony sprzęt został odebrany bez zastrzeżeń jako w pełni sprawny przez uprawnionych pracowników.*

Strona odbierająca stwierdza, że nie dokonała odbioru z przyczyn określonych w uwagach do protokołu.*

Protokół spisano w dwóch jednobrzmiących egzemplarzach.

Strona przekazująca: Strona odbierająca:

…… ……..

(Czytelny podpis i pieczęć) (Czytelny podpis i pieczęć)

Osoba materialnie odpowiedzialna

……

(Czytelny podpis i pieczęć)

UWAGI:

……

……

……

……

……

Strona przekazująca: Strona odbierająca:

…… ……..

(Czytelny podpis i pieczęć) (Czytelny podpis i pieczęć)

Osoba materialnie odpowiedzialna

……

(Czytelny podpis i pieczęć)

* *niepotrzebne skreślić*

STANDARDOWY FORMULARZ JEDNOLITEGO EUROPEJSKIEGO DOKUMENTU ZAMÓWIENIA

Część I: Informacje dotyczące postępowania o udzielenie zamówienia oraz instytucji zamawiającej lub podmiotu zamawiającego

W przypadku postępowań o udzielenie zamówienia, w ramach których zaproszenie do ubiegania się o zamówienie opublikowano w Dzienniku Urzędowym Unii Europejskiej, informacje wymagane w części I zostaną automatycznie wyszukane, pod warunkiem że do utworzenia i wypełnienia jednolitego europejskiego dokumentu zamówienia wykorzystany zostanie elektroniczny serwis poświęcony jednolitemu europejskiemu dokumentowi zamówienia[1]. **Adres publikacyjny stosownego ogłoszenia[2] w Dzienniku Urzędowym Unii Europejskiej:**

Dz.U. UE S numer [], data [], strona [],

Numer ogłoszenia w Dz.U. S: [ ][ ][ ][ ]/S [ ][ ][ ]–[ ][ ][ ][ ][ ][ ]

Jeżeli nie opublikowano zaproszenia do ubiegania się o zamówienie w Dz.U., instytucja zamawiająca lub podmiot zamawiający muszą wypełnić informacje umożliwiające jednoznaczne zidentyfikowanie postępowania o udzielenie zamówienia:

W przypadku gdy publikacja ogłoszenia w Dzienniku Urzędowym Unii Europejskiej nie jest wymagana, proszę podać inne informacje umożliwiające jednoznaczne zidentyfikowanie postępowania o udzielenie zamówienia (np. adres publikacyjny na poziomie krajowym): [….]

INFORMACJE NA TEMAT POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

Informacje wymagane w części I zostaną automatycznie wyszukane, pod warunkiem że wyżej wymieniony elektroniczny serwis poświęcony jednolitemu europejskiemu dokumentowi zamówienia zostanie wykorzystany do utworzenia i wypełnienia tego dokumentu. W przeciwnym przypadku informacje te musi wypełnić wykonawca.

Tożsamość zamawiającego[3]	**Odpowiedź:**
Nazwa:	*Uniwersytet Jana Kochanowskiego w Kielcach*
Jakiego zamówienia dotyczy niniejszy dokument?	***Odpowiedź:***
Tytuł lub krótki opis udzielanego zamówienia[4]:	***Dostawa oprogramowania antywirusowego wraz z konsolą do zarządzania."***
Numer referencyjny nadany sprawie przez instytucję zamawiającą lub podmiot zamawiający (*jeżeli dotyczy*)[5]:	*DP.2301.8. 2019*

Wszystkie pozostałe informacje we wszystkich sekcjach jednolitego europejskiego dokumentu zamówienia powinien wypełnić wykonawca.

[1] Służby Komisji udostępnią instytucjom zamawiającym, podmiotom zamawiającym, wykonawcom, dostawcom usług elektronicznych i innym zainteresowanym stronom bezpłatny elektroniczny serwis poświęcony jednolitemu europejskiemu dokumentowi zamówienia.

[2] W przypadku **instytucji zamawiających**: **wstępne ogłoszenie informacyjne** wykorzystywane jako zaproszenie do ubiegania się o zamówienie albo **ogłoszenie o zamówieniu**.
W przypadku **podmiotów zamawiających**: **okresowe ogłoszenie informacyjne** wykorzystywane jako zaproszenie do ubiegania się o zamówienie, **ogłoszenie o zamówieniu** lub **ogłoszenie o istnieniu systemu kwalifikowania**.

[3] Informacje te należy skopiować z sekcji I pkt I.1 stosownego ogłoszenia. W przypadku wspólnego zamówienia proszę podać nazwy wszystkich uczestniczących zamawiających.

[4] Zob. pkt II.1.1 i II.1.3 stosownego ogłoszenia.

[5] Zob. pkt II.1.1 stosownego ogłoszenia.

Część II: Informacje dotyczące wykonawcy

A: INFORMACJE NA TEMAT WYKONAWCY

Identyfikacja:	**Odpowiedź:**
Nazwa:	[ ]
Numer VAT, jeżeli dotyczy: Jeżeli numer VAT nie ma zastosowania, proszę podać inny krajowy numer identyfikacyjny, jeżeli jest wymagany i ma zastosowanie.	[ ] [ ]
Adres pocztowy:	[……]
Osoba lub osoby wyznaczone do kontaktów[6]: Telefon: Adres e-mail: Adres internetowy (adres www) (*jeżeli dotyczy*):	[……] [……] [……] [……]
Informacje ogólne:	**Odpowiedź:**
Czy wykonawca jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem[7]?	[] Tak [] Nie
<u>Jedynie w przypadku gdy zamówienie jest zastrzeżone[8]:</u> czy wykonawca jest zakładem pracy chronionej, „przedsiębiorstwem społecznym”[9] lub czy będzie realizował zamówienie w ramach programów zatrudnienia chronionego? **Jeżeli tak,** jaki jest odpowiedni odsetek pracowników niepełnosprawnych lub defaworyzowanych? Jeżeli jest to wymagane, proszę określić, do której kategorii lub których kategorii pracowników niepełnosprawnych lub defaworyzowanych należą dani pracownicy.	[] Tak [] Nie […] [….]
Jeżeli dotyczy, czy wykonawca jest wpisany do urzędowego wykazu zatwierdzonych wykonawców lub posiada równoważne	[] Tak [] Nie [] Nie dotyczy

[6] Proszę powtórzyć informacje dotyczące osób wyznaczonych do kontaktów tyle razy, ile jest to konieczne.

[7] Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych.
Mikroprzedsiębiorstwo: przedsiębiorstwo, które **zatrudnia mniej niż 10 osób** i którego roczny obrót lub roczna suma bilansowa **nie przekracza 2 milionów EUR**.
Małe przedsiębiorstwo: przedsiębiorstwo, które **zatrudnia mniej niż 50 osób** i którego roczny obrót lub roczna suma bilansowa **nie przekracza 10 milionów EUR**.
Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które **zatrudniają mniej niż 250 osób** i których **roczny obrót nie przekracza 50 milionów EUR *lub* roczna suma bilansowa nie przekracza 43 milionów EUR**.

[8] Zob. ogłoszenie o zamówieniu, pkt III.1.5.

[9] Tj. przedsiębiorstwem, którego głównym celem jest społeczna i zawodowa integracja osób niepełnosprawnych lub defaworyzowanych.

zaświadczenie (np. w ramach krajowego systemu (wstępnego) kwalifikowania)?	
Jeżeli tak: **Proszę udzielić odpowiedzi w pozostałych fragmentach niniejszej sekcji, w sekcji B i, w odpowiednich przypadkach, sekcji C niniejszej części, uzupełnić część V (w stosownych przypadkach) oraz w każdym przypadku wypełnić i podpisać część VI.** a) Proszę podać nazwę wykazu lub zaświadczenia i odpowiedni numer rejestracyjny lub numer zaświadczenia, jeżeli dotyczy: b) Jeżeli poświadczenie wpisu do wykazu lub wydania zaświadczenia jest dostępne w formie elektronicznej, proszę podać: c) Proszę podać dane referencyjne stanowiące podstawę wpisu do wykazu lub wydania zaświadczenia oraz, w stosownych przypadkach, klasyfikację nadaną w urzędowym wykazie[10]: d) Czy wpis do wykazu lub wydane zaświadczenie obejmują wszystkie wymagane kryteria kwalifikacji? **Jeżeli nie:** **Proszę dodatkowo uzupełnić brakujące informacje w części IV w sekcjach A, B, C lub D, w zależności od przypadku.** **WYŁĄCZNIE jeżeli jest to wymagane w stosownym ogłoszeniu lub dokumentach zamówienia:** e) Czy wykonawca będzie w stanie przedstawić zaświadczenie odnoszące się do płatności składek na ubezpieczenie społeczne i podatków lub przedstawić informacje, które umożliwią instytucji zamawiającej lub podmiotowi zamawiającemu uzyskanie tego zaświadczenia bezpośrednio za pomocą bezpłatnej krajowej bazy danych w dowolnym państwie członkowskim? Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	a) [……] b) (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……][……] c) [……] d) [] Tak [] Nie e) [] Tak [] Nie (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……][……]
Rodzaj uczestnictwa:	**Odpowiedź:**
Czy wykonawca bierze udział w postępowaniu o udzielenie zamówienia wspólnie z innymi wykonawcami[11]?	[] Tak [] Nie
Jeżeli tak, proszę dopilnować, aby pozostali uczestnicy przedstawili odrębne jednolite europejskie dokumenty zamówienia.	
Jeżeli tak: a) Proszę wskazać rolę wykonawcy w grupie (lider, odpowiedzialny za określone zadania itd.): b) Proszę wskazać pozostałych wykonawców	a): [……]

[10] Dane referencyjne i klasyfikacja, o ile istnieją, są określone na zaświadczeniu.

[11] Zwłaszcza w ramach grupy, konsorcjum, spółki *joint venture* lub podobnego podmiotu.

biorących wspólnie udział w postępowaniu o udzielenie zamówienia: c) W stosownych przypadkach nazwa grupy biorącej udział:	b): [……] c): [……]
Części	**Odpowiedź:**
W stosownych przypadkach wskazanie części zamówienia, w odniesieniu do której (których) wykonawca zamierza złożyć ofertę.	[ ]

B: INFORMACJE NA TEMAT PRZEDSTAWICIELI WYKONAWCY

W stosownych przypadkach proszę podać imię i nazwisko (imiona i nazwiska) oraz adres(-y) osoby (osób) upoważnionej(-ych) do reprezentowania wykonawcy na potrzeby niniejszego postępowania o udzielenie zamówienia:

Osoby upoważnione do reprezentowania, o ile istnieją:	**Odpowiedź:**
Imię i nazwisko, wraz z datą i miejscem urodzenia, jeżeli są wymagane:	[……], [……]
Stanowisko/Działający(-a) jako:	[……]
Adres pocztowy:	[……]
Telefon:	[……]
Adres e-mail:	[……]
W razie potrzeby proszę podać szczegółowe informacje dotyczące przedstawicielstwa (jego form, zakresu, celu itd.):	[……]

C: INFORMACJE NA TEMAT POLEGANIA NA ZDOLNOŚCI INNYCH PODMIOTÓW

Zależność od innych podmiotów:	**Odpowiedź:**
Czy wykonawca polega na zdolności innych podmiotów w celu spełnienia kryteriów kwalifikacji określonych poniżej w części IV oraz (ewentualnych) kryteriów i zasad określonych poniżej w części V?	[] Tak [] Nie

Jeżeli tak, proszę przedstawić – **dla każdego** z podmiotów, których to dotyczy – odrębny formularz jednolitego europejskiego dokumentu zamówienia zawierający informacje wymagane w **niniejszej części sekcja A i B oraz w części III**, należycie wypełniony i podpisany przez dane podmioty.
Należy zauważyć, że dotyczy to również wszystkich pracowników technicznych lub służb technicznych, nienależących bezpośrednio do przedsiębiorstwa danego wykonawcy, w szczególności tych odpowiedzialnych za kontrolę jakości, a w przypadku zamówień publicznych na roboty budowlane – tych, do których wykonawca będzie mógł się zwrócić o wykonanie robót budowlanych.
O ile ma to znaczenie dla określonych zdolności, na których polega wykonawca, proszę dołączyć – dla każdego z podmiotów, których to dotyczy – informacje wymagane w częściach IV i V[12].

[12] Np. dla służb technicznych zaangażowanych w kontrolę jakości: część IV, sekcja C, pkt 3.

D: INFORMACJE DOTYCZĄCE PODWYKONAWCÓW, NA KTÓRYCH ZDOLNOŚCI WYKONAWCA NIE POLEGA

(Sekcja, którą należy wypełnić jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający wprost tego zażąda.)

Podwykonawstwo:	**Odpowiedź:**
Czy wykonawca zamierza zlecić osobom trzecim podwykonawstwo jakiejkolwiek części zamówienia?	[] Tak [] Nie Jeżeli **tak i o ile jest to wiadome**, proszę podać wykaz proponowanych podwykonawców: […]

Jeżeli instytucja zamawiająca lub podmiot zamawiający wyraźnie żąda przedstawienia tych informacji oprócz informacji **wymaganych w niniejszej sekcji, proszę przedstawić – dla każdego podwykonawcy (każdej kategorii podwykonawców), których to dotyczy – informacje wymagane w niniejszej części sekcja A i B oraz w części III.**

Część III: Podstawy wykluczenia

A: PODSTAWY ZWIĄZANE Z WYROKAMI SKAZUJĄCYMI ZA PRZESTĘPSTWO

W art. 57 ust. 1 dyrektywy 2014/24/UE określono następujące powody wykluczenia:

1. udział w **organizacji przestępczej**[13];

korupcja[14];

nadużycie finansowe[15];

przestępstwa terrorystyczne lub przestępstwa związane z działalnością terrorystyczną[16]

pranie pieniędzy lub finansowanie terroryzmu[17]

praca dzieci i inne formy **handlu ludźmi**[18].

Podstawy związane z wyrokami skazującymi za przestępstwo na podstawie przepisów krajowych stanowiących wdrożenie podstaw określonych w art. 57 ust. 1 wspomnianej dyrektywy:	**Odpowiedź:**
Czy w stosunku do **samego wykonawcy** bądź **jakiejkolwiek** osoby będącej członkiem organów administracyjnych, zarządzających lub nadzorczych wykonawcy, lub posiadającej w	[] Tak [] Nie Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać: (adres internetowy, wydający

[13] Zgodnie z definicją zawartą w art. 2 decyzji ramowej Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej (Dz.U. L 300 z 11.11.2008, s. 42).

[14] Zgodnie z definicją zawartą w art. 3 Konwencji w sprawie zwalczania korupcji urzędników Wspólnot Europejskich i urzędników państw członkowskich Unii Europejskiej (Dz.U. C 195 z 25.6.1997, s. 1) i w art. 2 ust. 1 decyzji ramowej Rady 2003/568/WSiSW z dnia 22 lipca 2003 r. w sprawie zwalczania korupcji w sektorze prywatnym (Dz.U. L 192 z 31.7.2003, s. 54). Ta podstawa wykluczenia obejmuje również korupcję zdefiniowaną w prawie krajowym instytucji zamawiającej (podmiotu zamawiającego) lub wykonawcy.

[15] W rozumieniu art. 1 Konwencji w sprawie ochrony interesów finansowych Wspólnot Europejskich (Dz.U. C 316 z 27.11.1995, s. 48).

[16] Zgodnie z definicją zawartą w art. 1 i 3 decyzji ramowej Rady z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (Dz.U. L 164 z 22.6.2002, s. 3). Ta podstawa wykluczenia obejmuje również podżeganie do popełnienia przestępstwa, pomocnictwo, współsprawstwo lub usiłowanie popełnienia przestępstwa, o których mowa w art. 4 tejże decyzji ramowej.

[17] Zgodnie z definicją zawartą w art. 1 dyrektywy 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu (Dz.U. L 309 z 25.11.2005, s. 15).

[18] Zgodnie z definicją zawartą w art. 2 dyrektywy Parlamentu Europejskiego i Rady 2011/36/UE z dnia 5 kwietnia 2011 r. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępującej decyzję ramową Rady 2002/629/WSiSW (Dz.U. L 101 z 15.4.2011, s. 1).

przedsiębiorstwie wykonawcy uprawnienia do reprezentowania, uprawnienia decyzyjne lub kontrolne, **wydany został prawomocny wyrok** z jednego z wyżej wymienionych powodów, orzeczeniem sprzed najwyżej pięciu lat lub w którym okres wykluczenia określony bezpośrednio w wyroku nadal obowiązuje?	urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……][……][19]
Jeżeli tak, proszę podać[20]: a) datę wyroku, określić, których spośród punktów 1–6 on dotyczy, oraz podać powód(-ody) skazania; b) wskazać, kto został skazany [ ]; **c) w zakresie, w jakim zostało to bezpośrednio ustalone w wyroku:**	a) data: [ ], punkt(-y): [ ], powód(-ody): [ ] b) [……] c) długość okresu wykluczenia [……] oraz punkt(-y), którego(-ych) to dotyczy. Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać: (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……][……][21]
W przypadku skazania, czy wykonawca przedsięwziął środki w celu wykazania swojej rzetelności pomimo istnienia odpowiedniej podstawy wykluczenia[22] („samooczyszczenie")?	[] Tak [] Nie
Jeżeli tak, proszę opisać przedsięwzięte środki[23]:	[……]

B: PODSTAWY ZWIĄZANE Z PŁATNOŚCIĄ PODATKÓW LUB SKŁADEK NA UBEZPIECZENIE SPOŁECZNE

Płatność podatków lub składek na ubezpieczenie społeczne:	**Odpowiedź:**	
Czy wykonawca wywiązał się ze wszystkich **obowiązków dotyczących płatności podatków lub składek na ubezpieczenie społeczne**, zarówno w państwie, w którym ma siedzibę, jak i w państwie członkowskim instytucji zamawiającej lub podmiotu zamawiającego, jeżeli jest ono inne niż państwo siedziby?	[] Tak [] Nie	
	Podatki	**Składki na ubezpieczenia społeczne**
Jeżeli nie, proszę wskazać: a) państwo lub państwo członkowskie, którego to dotyczy; b) jakiej kwoty to dotyczy? c) w jaki sposób zostało ustalone to naruszenie obowiązków: 1) w trybie **decyzji** sądowej lub administracyjnej:	a) [……] b) [……] c1) [] Tak [] Nie [] Tak [] Nie	a) [……] b) [……] c1) [] Tak [] Nie – [] Tak [] Nie

[19] Proszę powtórzyć tyle razy, ile jest to konieczne.
[20] Proszę powtórzyć tyle razy, ile jest to konieczne.
[21] Proszę powtórzyć tyle razy, ile jest to konieczne.
[22] Zgodnie z przepisami krajowymi wdrażającymi art. 57 ust. 6 dyrektywy 2014/24/UE.
[23] Uwzględniając charakter popełnionych przestępstw (jednorazowe, powtarzające się, systematyczne itd.), objaśnienie powinno wykazywać stosowność przedsięwziętych środków.

Czy ta decyzja jest ostateczna i wiążąca? – Proszę podać datę wyroku lub decyzji. – W przypadku wyroku, **o ile została w nim bezpośrednio określona**, długość okresu wykluczenia: 2) w **inny sposób**? Proszę sprecyzować, w jaki: d) Czy wykonawca spełnił lub spełni swoje obowiązki, dokonując płatności należnych podatków lub składek na ubezpieczenie społeczne, lub też zawierając wiążące porozumienia w celu spłaty tych należności, obejmujące w stosownych przypadkach narosłe odsetki lub grzywny?	– [……] – [……] c2) […] d) [] Tak [] Nie **Jeżeli tak**, proszę podać szczegółowe informacje na ten temat: [……]	– [……] – [……] c2) […] d) [] Tak [] Nie **Jeżeli tak**, proszę podać szczegółowe informacje na ten temat: [……]
Jeżeli odnośna dokumentacja dotycząca płatności podatków lub składek na ubezpieczenie społeczne jest dostępna w formie elektronicznej, proszę wskazać:	(adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [24] [……][……][……]	

C: PODSTAWY ZWIĄZANE Z NIEWYPŁACALNOŚCIĄ, KONFLIKTEM INTERESÓW LUB WYKROCZENIAMI ZAWODOWYMI[25]

Należy zauważyć, że do celów niniejszego zamówienia niektóre z poniższych podstaw wykluczenia mogą być zdefiniowane bardziej precyzyjnie w prawie krajowym, w stosownym ogłoszeniu lub w dokumentach zamówienia. Tak więc prawo krajowe może na przykład stanowić, że pojęcie „poważnego wykroczenia zawodowego" może obejmować kilka różnych postaci zachowania stanowiącego wykroczenie.

Informacje dotyczące ewentualnej niewypłacalności, konfliktu interesów lub wykroczeń zawodowych	**Odpowiedź:**
Czy wykonawca, **wedle własnej wiedzy**, naruszył **swoje obowiązki** w dziedzinie **prawa środowiska, prawa socjalnego i prawa pracy**[26]?	[] Tak [] Nie
	Jeżeli tak, czy wykonawca przedsięwziął środki w celu wykazania swojej rzetelności pomimo istnienia odpowiedniej podstawy wykluczenia („samooczyszczenie")? [] Tak [] Nie **Jeżeli tak**, proszę opisać przedsięwzięte środki: [……]
Czy wykonawca znajduje się w jednej z następujących sytuacji: a) **zbankrutował**; lub b) **prowadzone jest wobec niego postępowanie upadłościowe** lub likwidacyjne; lub c) zawarł **układ z wierzycielami**; lub d) znajduje się w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej	[] Tak [] Nie

[24] Proszę powtórzyć tyle razy, ile jest to konieczne.
[25] Zob. art. 57 ust. 4 dyrektywy 2014/24/WE.
[26] O których mowa, do celów niniejszego zamówienia, w prawie krajowym, w stosownym ogłoszeniu lub w dokumentach zamówienia bądź w art. 18 ust. 2 dyrektywy 2014/24/UE.

w krajowych przepisach ustawowych i wykonawczych[27]; lub e) jego aktywami zarządza likwidator lub sąd; lub f) jego działalność gospodarcza jest zawieszona? **Jeżeli tak:** – Proszę podać szczegółowe informacje: – Proszę podać powody, które pomimo powyższej sytuacji umożliwiają realizację zamówienia, z uwzględnieniem mających zastosowanie przepisów krajowych i środków dotyczących kontynuowania działalności gospodarczej[28]. Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	– [……] – [……] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
Czy wykonawca jest winien **poważnego wykroczenia zawodowego**[29]? Jeżeli tak, proszę podać szczegółowe informacje na ten temat:	[] Tak [] Nie [……]
	Jeżeli tak, czy wykonawca przedsięwziął środki w celu samooczyszczenia? [] Tak [] Nie **Jeżeli tak**, proszę opisać przedsięwzięte środki: [……]
Czy wykonawca zawarł z innymi wykonawcami **porozumienia mające na celu zakłócenie konkurencji**? **Jeżeli tak**, proszę podać szczegółowe informacje na ten temat:	[] Tak [] Nie […]
	Jeżeli tak, czy wykonawca przedsięwziął środki w celu samooczyszczenia? [] Tak [] Nie **Jeżeli tak**, proszę opisać przedsięwzięte środki: [……]
Czy wykonawca wie o jakimkolwiek **konflikcie interesów**[30] spowodowanym jego udziałem w postępowaniu o udzielenie zamówienia? **Jeżeli tak**, proszę podać szczegółowe informacje na ten temat:	[] Tak [] Nie […]
Czy wykonawca lub przedsiębiorstwo związane z wykonawcą **doradzał(-o)** instytucji zamawiającej lub podmiotowi zamawiającemu bądź był(-o) w inny sposób **zaangażowany(-e) w przygotowanie** postępowania o udzielenie zamówienia? **Jeżeli tak**, proszę podać szczegółowe informacje na ten temat:	[] Tak [] Nie […]

[27] Zob. przepisy krajowe, stosowne ogłoszenie lub dokumenty zamówienia.

[28] Nie trzeba podawać tych informacji, jeżeli wykluczenie wykonawców w jednym z przypadków wymienionych w lit. a)–f) stało się obowiązkowe na mocy obowiązującego prawa krajowego bez żadnej możliwości odstępstwa w sytuacji, gdy wykonawcy są pomimo to w stanie zrealizować zamówienie.

[29] W stosownych przypadkach zob. definicje w prawie krajowym, stosownym ogłoszeniu lub dokumentach zamówienia.

[30] Wskazanym w prawie krajowym, stosownym ogłoszeniu lub dokumentach zamówienia.

Czy wykonawca znajdował się w sytuacji, w której wcześniejsza umowa w sprawie zamówienia publicznego, wcześniejsza umowa z podmiotem zamawiającym lub wcześniejsza umowa w sprawie koncesji została **rozwiązana przed czasem**, lub w której nałożone zostało odszkodowanie bądź inne porównywalne sankcje w związku z tą wcześniejszą umową? **Jeżeli tak**, proszę podać szczegółowe informacje na ten temat:	[] Tak [] Nie […]
	Jeżeli tak, czy wykonawca przedsięwziął środki w celu samooczyszczenia? [] Tak [] Nie **Jeżeli tak**, proszę opisać przedsięwzięte środki: [……]
Czy wykonawca może potwierdzić, że: nie jest winny poważnego **wprowadzenia w błąd** przy dostarczaniu informacji wymaganych do weryfikacji braku podstaw wykluczenia lub do weryfikacji spełnienia kryteriów kwalifikacji; b) nie **zataił** tych informacji; c) jest w stanie niezwłocznie przedstawić dokumenty potwierdzające wymagane przez instytucję zamawiającą lub podmiot zamawiający; oraz d) nie przedsięwziął kroków, aby w bezprawny sposób wpłynąć na proces podejmowania decyzji przez instytucję zamawiającą lub podmiot zamawiający, pozyskać informacje poufne, które mogą dać mu nienależną przewagę w postępowaniu o udzielenie zamówienia, lub wskutek zaniedbania przedstawić wprowadzające w błąd informacje, które mogą mieć istotny wpływ na decyzje w sprawie wykluczenia, kwalifikacji lub udzielenia zamówienia?	[] Tak [] Nie

D: INNE PODSTAWY WYKLUCZENIA, KTÓRE MOGĄ BYĆ PRZEWIDZIANE W PRZEPISACH KRAJOWYCH PAŃSTWA CZŁONKOWSKIEGO INSTYTUCJI ZAMAWIAJĄCEJ LUB PODMIOTU ZAMAWIAJĄCEGO

Podstawy wykluczenia o charakterze wyłącznie krajowym	**Odpowiedź:**
Czy mają zastosowanie **podstawy wykluczenia o charakterze wyłącznie krajowym** określone w stosownym ogłoszeniu lub w dokumentach zamówienia? Jeżeli dokumentacja wymagana w stosownym ogłoszeniu lub w dokumentach zamówienia jest dostępna w formie elektronicznej, proszę wskazać:	[] Tak [] Nie (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……][31]
W przypadku gdy ma zastosowanie którakolwiek z podstaw wykluczenia o charakterze wyłącznie krajowym, czy wykonawca przedsięwziął środki w celu samooczyszczenia? **Jeżeli tak**, proszę opisać przedsięwzięte środki:	[] Tak [] Nie [……]

[31] Proszę powtórzyć tyle razy, ile jest to konieczne.

Część IV: Kryteria kwalifikacji

W odniesieniu do kryteriów kwalifikacji (sekcja α lub sekcje A–D w niniejszej części) wykonawca oświadcza, że:

α: OGÓLNE OŚWIADCZENIE DOTYCZĄCE WSZYSTKICH KRYTERIÓW KWALIFIKACJI

Wykonawca powinien wypełnić to pole jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający wskazały w stosownym ogłoszeniu lub w dokumentach zamówienia, o których mowa w ogłoszeniu, że wykonawca może ograniczyć się do wypełnienia sekcji α w części IV i nie musi wypełniać żadnej z pozostałych sekcji w części IV:

Spełnienie wszystkich wymaganych kryteriów kwalifikacji	**Odpowiedź**
Spełnia wymagane kryteria kwalifikacji:	[] Tak [] Nie

A: KOMPETENCJE

Wykonawca powinien przedstawić informacje jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający wymagają danych kryteriów kwalifikacji w stosownym ogłoszeniu lub w dokumentach zamówienia, o których mowa w ogłoszeniu.

Kompetencje	**Odpowiedź**
1) Figuruje w odpowiednim rejestrze zawodowym lub handlowym prowadzonym w państwie członkowskim siedziby wykonawcy[32]: Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	[…] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
2) W odniesieniu do zamówień publicznych na usługi: Czy konieczne jest **posiadanie** określonego **zezwolenia lub bycie członkiem** określonej organizacji, aby mieć możliwość świadczenia usługi, o której mowa, w państwie siedziby wykonawcy? Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	[] Tak [] Nie Jeżeli tak, proszę określić, o jakie zezwolenie lub status członkowski chodzi, i wskazać, czy wykonawca je posiada: […] [] Tak [] Nie (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]

B: SYTUACJA EKONOMICZNA I FINANSOWA

Wykonawca powinien przedstawić informacje jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający wymagają danych kryteriów kwalifikacji w stosownym ogłoszeniu lub w dokumentach zamówienia, o których mowa w ogłoszeniu.

Sytuacja ekonomiczna i finansowa	**Odpowiedź:**
1a) Jego („ogólny”) **roczny obrót** w ciągu określonej liczby lat obrotowych wymaganej w stosownym ogłoszeniu lub dokumentach zamówienia jest następujący**:**	rok: [……] obrót: [……] […] waluta rok: [……] obrót: [……] […] waluta rok: [……] obrót: [……] […] waluta

[32] Zgodnie z opisem w załączniku XI do dyrektywy 2014/24/UE; wykonawcy z niektórych państw członkowskich mogą być zobowiązani do spełnienia innych wymogów określonych w tym załączniku.

i/lub 1b) Jego **średni** roczny **obrót w ciągu określonej liczby lat wymaganej w stosownym ogłoszeniu lub dokumentach zamówienia jest następujący[33] ():** Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	(liczba lat, średni obrót)**:** [……], [……] […] waluta (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
2a) Jego roczny („specyficzny”) **obrót w obszarze działalności gospodarczej objętym zamówieniem** i określonym w stosownym ogłoszeniu lub dokumentach zamówienia w ciągu wymaganej liczby lat obrotowych jest następujący: **i/lub** 2b) Jego **średni** roczny **obrót w przedmiotowym obszarze i w ciągu określonej liczby lat wymaganej w stosownym ogłoszeniu lub dokumentach zamówienia jest następujący[34]:** Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	rok: [……] obrót: [……] […] waluta rok: [……] obrót: [……] […] waluta rok: [……] obrót: [……] […] waluta (liczba lat, średni obrót)**:** [……], [……] […] waluta (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
3) W przypadku gdy informacje dotyczące obrotu (ogólnego lub specyficznego) nie są dostępne za cały wymagany okres, proszę podać datę założenia przedsiębiorstwa wykonawcy lub rozpoczęcia działalności przez wykonawcę:	[……]
4) W odniesieniu do **wskaźników finansowych[35]** określonych w stosownym ogłoszeniu lub dokumentach zamówienia wykonawca oświadcza, że aktualna(-e) wartość(-ci) wymaganego(-ych) wskaźnika(-ów) jest (są) następująca(-e): Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	(określenie wymaganego wskaźnika – stosunek X do Y[36] – oraz wartość): [……], [……][37] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
5) W ramach **ubezpieczenia z tytułu ryzyka zawodowego** wykonawca jest ubezpieczony na następującą kwotę: Jeżeli te informacje są dostępne w formie elektronicznej, proszę wskazać:	[……] […] waluta (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
6) W odniesieniu do **innych ewentualnych wymogów ekonomicznych lub finansowych**, które mogły zostać określone w stosownym ogłoszeniu lub dokumentach zamówienia, wykonawca oświadcza, że Jeżeli odnośna dokumentacja, która **mogła** zostać określona w stosownym ogłoszeniu lub w dokumentach zamówienia, jest dostępna w formie elektronicznej, proszę wskazać:	[…….] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]

33 Jedynie jeżeli jest to dopuszczone w stosownym ogłoszeniu lub dokumentach zamówienia.
34 Jedynie jeżeli jest to dopuszczone w stosownym ogłoszeniu lub dokumentach zamówienia.
35 Np. stosunek aktywów do zobowiązań.
36 Np. stosunek aktywów do zobowiązań.
37 Proszę powtórzyć tyle razy, ile jest to konieczne.

C: ZDOLNOŚĆ TECHNICZNA I ZAWODOWA

Wykonawca powinien przedstawić informacje jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający wymagają danych kryteriów kwalifikacji w stosownym ogłoszeniu lub w dokumentach zamówienia, o których mowa w ogłoszeniu.

<table>
<tr><th>Zdolność techniczna i zawodowa</th><th>Odpowiedź:</th></tr>
<tr><td>1a) Jedynie w odniesieniu do zamówień publicznych na roboty budowlane:
W okresie odniesienia[38] wykonawca wykonał następujące roboty budowlane określonego rodzaju:
Jeżeli odnośna dokumentacja dotycząca zadowalającego wykonania i rezultatu w odniesieniu do najważniejszych robót budowlanych jest dostępna w formie elektronicznej, proszę wskazać:</td><td>Liczba lat (okres ten został wskazany w stosownym ogłoszeniu lub dokumentach zamówienia): […]
Roboty budowlane: [……]

(adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]</td></tr>
<tr><td>1b) Jedynie w odniesieniu do zamówień publicznych na dostawy i zamówień publicznych na usługi:
W okresie odniesienia[39] wykonawca zrealizował następujące główne dostawy określonego rodzaju lub wyświadczył następujące główne usługi określonego rodzaju: Przy sporządzaniu wykazu proszę podać kwoty, daty i odbiorców, zarówno publicznych, jak i prywatnych[40]:</td><td>Liczba lat (okres ten został wskazany w stosownym ogłoszeniu lub dokumentach zamówienia): […]
<table><tr><th>Opis</th><th>Kwoty</th><th>Daty</th><th>Odbiorcy</th></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>2) Może skorzystać z usług następujących pracowników technicznych lub służb technicznych[41], w szczególności tych odpowiedzialnych za kontrolę jakości:
W przypadku zamówień publicznych na roboty budowlane wykonawca będzie mógł się zwrócić do następujących pracowników technicznych lub służb technicznych o wykonanie robót:</td><td>[……]

[……]</td></tr>
<tr><td>3) Korzysta z następujących urządzeń technicznych oraz środków w celu zapewnienia jakości, a jego zaplecze naukowo-badawcze jest następujące:</td><td>[……]</td></tr>
<tr><td>4) Podczas realizacji zamówienia będzie mógł stosować następujące systemy zarządzania łańcuchem dostaw i śledzenia łańcucha dostaw:</td><td>[……]</td></tr>
<tr><td>5) W odniesieniu do produktów lub usług o złożonym charakterze, które mają zostać dostarczone, lub – wyjątkowo – w odniesieniu do produktów lub usług o szczególnym</td><td></td></tr>
</table>

[38] Instytucje zamawiające mogą **wymagać**, aby okres ten wynosił do pięciu lat, i **dopuszczać** legitymowanie się doświadczeniem sprzed **ponad** pięciu lat.

[39] Instytucje zamawiające mogą **wymagać**, aby okres ten wynosił do trzech lat, i **dopuszczać** legitymowanie się doświadczeniem sprzed **ponad** trzech lat.

[40] Innymi słowy, należy wymienić **wszystkich** odbiorców, a wykaz powinien obejmować zarówno klientów publicznych, jak i prywatnych w odniesieniu do przedmiotowych dostaw lub usług.

[41] W przypadku pracowników technicznych lub służb technicznych nienależących bezpośrednio do przedsiębiorstwa danego wykonawcy, lecz na których zdolności wykonawca ten polega, jak określono w części II sekcja C, należy wypełnić odrębne formularze jednolitego europejskiego dokumentu zamówienia.

przeznaczeniu: Czy wykonawca **zezwoli** na przeprowadzenie **kontroli**[42] swoich **zdolności produkcyjnych** lub **zdolności technicznych**, a w razie konieczności także dostępnych mu **środków naukowych i badawczych**, jak również **środków kontroli jakości**?	[] Tak [] Nie
6) Następującym **wykształceniem i kwalifikacjami zawodowymi** legitymuje się: a) sam usługodawca lub wykonawca: **lub** (w zależności od wymogów określonych w stosownym ogłoszeniu lub dokumentach zamówienia): b) jego kadra kierownicza:	a) [……] b) [……]
7) Podczas realizacji zamówienia wykonawca będzie mógł stosować następujące **środki zarządzania środowiskowego**:	[……]
8) Wielkość **średniego rocznego zatrudnienia** u wykonawcy oraz liczebność kadry kierowniczej w ostatnich trzech latach są następujące	Rok, średnie roczne zatrudnienie: [……], [……] [……], [……] [……], [……] Rok, liczebność kadry kierowniczej: [……], [……] [……], [……] [……], [……]
9) Będzie dysponował następującymi **narzędziami, wyposażeniem zakładu i urządzeniami technicznymi** na potrzeby realizacji zamówienia:	[……]
10) Wykonawca **zamierza ewentualnie zlecić podwykonawcom**[43] następującą **część (procentową)** zamówienia:	[……]
11) W odniesieniu do **zamówień publicznych na dostawy**: Wykonawca dostarczy wymagane próbki, opisy lub fotografie produktów, które mają być dostarczone i którym nie musi towarzyszyć świadectwo autentyczności. Wykonawca oświadcza ponadto, że w stosownych przypadkach przedstawi wymagane świadectwa autentyczności. Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	[] Tak [] Nie [] Tak [] Nie (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
12) W odniesieniu do **zamówień publicznych na dostawy**: Czy wykonawca może przedstawić wymagane **zaświadczenia** sporządzone przez urzędowe	[] Tak [] Nie

[42] Kontrolę ma przeprowadzać instytucja zamawiająca lub – w przypadku gdy instytucja ta wyrazi na to zgodę – w jej imieniu, właściwy organ urzędowy państwa, w którym dostawca lub usługodawca ma siedzibę.

[43] Należy zauważyć, że jeżeli wykonawca **postanowił** zlecić podwykonawcom realizację części zamówienia **oraz** polega na zdolności podwykonawców na potrzeby realizacji tej części, to należy wypełnić odrębny jednolity europejski dokument zamówienia dla tych podwykonawców (zob. powyżej, część II sekcja C).

instytuty lub agencje **kontroli jakości** o uznanych kompetencjach, potwierdzające zgodność produktów poprzez wyraźne odniesienie do specyfikacji technicznych lub norm, które zostały określone w stosownym ogłoszeniu lub dokumentach zamówienia? **Jeżeli nie**, proszę wyjaśnić dlaczego, i wskazać, jakie inne środki dowodowe mogą zostać przedstawione: Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	[…] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]

D: SYSTEMY ZAPEWNIANIA JAKOŚCI I NORMY ZARZĄDZANIA ŚRODOWISKOWEGO

Wykonawca powinien przedstawić informacje jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający wymagają systemów zapewniania jakości lub norm zarządzania środowiskowego w stosownym ogłoszeniu lub w dokumentach zamówienia, o których mowa w ogłoszeniu.

Systemy zapewniania jakości i normy zarządzania środowiskowego	**Odpowiedź:**
Czy wykonawca będzie w stanie przedstawić **zaświadczenia** sporządzone przez niezależne jednostki, poświadczające spełnienie przez wykonawcę wymaganych **norm zapewniania jakości**, w tym w zakresie dostępności dla osób niepełnosprawnych? **Jeżeli nie**, proszę wyjaśnić dlaczego, i określić, jakie inne środki dowodowe dotyczące systemu zapewniania jakości mogą zostać przedstawione: Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	[] Tak [] Nie [……] [……] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]
Czy wykonawca będzie w stanie przedstawić **zaświadczenia** sporządzone przez niezależne jednostki, poświadczające spełnienie przez wykonawcę wymogów określonych **systemów lub norm zarządzania środowiskowego**? **Jeżeli nie**, proszę wyjaśnić dlaczego, i określić, jakie inne środki dowodowe dotyczące **systemów lub norm zarządzania środowiskowego** mogą zostać przedstawione: Jeżeli odnośna dokumentacja jest dostępna w formie elektronicznej, proszę wskazać:	[] Tak [] Nie [……] [……] (adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……]

Część V: Ograniczanie liczby kwalifikujących się kandydatów

Wykonawca powinien przedstawić informacje jedynie w przypadku gdy instytucja zamawiająca lub podmiot zamawiający określiły obiektywne i niedyskryminacyjne kryteria lub zasady, które mają być stosowane w celu ograniczenia liczby kandydatów, którzy zostaną zaproszeni do złożenia ofert lub prowadzenia dialogu. Te informacje, którym mogą towarzyszyć wymogi dotyczące (rodzajów) zaświadczeń lub rodzajów dowodów w formie dokumentów, które ewentualnie należy przedstawić, określono w stosownym ogłoszeniu lub w dokumentach zamówienia, o których mowa w ogłoszeniu.
Dotyczy jedynie procedury ograniczonej, procedury konkurencyjnej z negocjacjami, dialogu konkurencyjnego i partnerstwa innowacyjnego:

Wykonawca oświadcza, że:

Ograniczanie liczby kandydatów	**Odpowiedź:**
W następujący sposób **spełnia** obiektywne i niedyskryminacyjne kryteria lub zasady, które mają być stosowane w celu ograniczenia liczby kandydatów:	[….]
W przypadku gdy wymagane są określone zaświadczenia lub inne rodzaje dowodów w formie dokumentów, proszę wskazać dla **każdego** z nich, czy wykonawca posiada wymagane dokumenty:	[] Tak [] Nie[45]
Jeżeli niektóre z tych zaświadczeń lub rodzajów dowodów w formie dokumentów są dostępne w postaci elektronicznej[44], proszę wskazać dla **każdego** z nich:	(adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji): [……][……][……][46]

Część VI: Oświadczenia końcowe

Niżej podpisany(-a)(-i) oficjalnie oświadcza(-ją), że informacje podane powyżej w częściach II–V są dokładne i prawidłowe oraz że zostały przedstawione z pełną świadomością konsekwencji poważnego wprowadzenia w błąd.

Niżej podpisany(-a)(-i) oficjalnie oświadcza(-ją), że jest (są) w stanie, na żądanie i bez zwłoki, przedstawić zaświadczenia i inne rodzaje dowodów w formie dokumentów, z wyjątkiem przypadków, w których:

a) instytucja zamawiająca lub podmiot zamawiający ma możliwość uzyskania odpowiednich dokumentów potwierdzających bezpośrednio za pomocą bezpłatnej krajowej bazy danych w dowolnym państwie członkowskim[47], lub

b) najpóźniej od dnia 18 kwietnia 2018 r.[48], instytucja zamawiająca lub podmiot zamawiający już posiada odpowiednią dokumentację.

Niżej podpisany(-a)(-i) oficjalnie wyraża(-ją) zgodę na to, aby [wskazać instytucję zamawiającą lub podmiot zamawiający określone w części I, sekcja A] uzyskał(-a)(-o) dostęp do dokumentów potwierdzających informacje, które zostały przedstawione w [wskazać część/sekcję/punkt(-y), których to dotyczy] niniejszego jednolitego europejskiego dokumentu zamówienia, na potrzeby [określić postępowanie o udzielenie zamówienia: (skrócony opis, adres publikacyjny w *Dzienniku Urzędowym Unii Europejskiej*, numer referencyjny)].

Data, miejscowość oraz – jeżeli jest to wymagane lub konieczne – podpis(-y): [……]

[44] Proszę jasno wskazać, do której z pozycji odnosi się odpowiedź.
[45] Proszę powtórzyć tyle razy, ile jest to konieczne.
[46] Proszę powtórzyć tyle razy, ile jest to konieczne.
[47] Pod warunkiem że wykonawca przekazał niezbędne informacje (adres internetowy, dane wydającego urzędu lub organu, dokładne dane referencyjne dokumentacji) umożliwiające instytucji zamawiającej lub podmiotowi zamawiającemu tę czynność. W razie potrzeby musi temu towarzyszyć odpowiednia zgoda na uzyskanie takiego dostępu.
[48] W zależności od wdrożenia w danym kraju artykułu 59 ust. 5 akapit drugi dyrektywy 2014/24/UE.

Załącznik nr 5 do SIWZ

.....

(nazwa /firma i dokładny adres Wykonawcy)

Wykaz dostaw

Postępowanie pn. „***Dostawa oprogramowania antywirusowego wraz z konsolą do zarządzania.”*** oznaczenie postępowania : DP.2301. ……. 2019

Oświadczam, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, (a jeżeli okres prowadzenia działalności jest krótszy- w tym okresie) zrealizowałem następujące dostawy

L.p.	Przedmiot dostawy oraz Podmiot na rzecz którego dostawa została wykonana	Data wykonania	Wartość
1	……		
2	……		
3	……		

Dokumenty potwierdzające, że dostawa została wykonana lub jest wykonywana należycie w załączeniu

…… , dnia …….. r.

……

Pieczątka i podpis/y osoby/osób uprawnionych

do składania oświadczeń woli w imieniu Wykonawcy

Załącznik nr 6 do SIWZ

Zgodnie z art. 24 ust. 11 ustawy PZP, Wykonawca, w terminie 3 dni od zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w ust. 1 pkt. 23

OŚWIADCZENIE

(DOT. GRUPY KAPITAŁOWEJ)

Postępowanie pn. „***Dostawa oprogramowania antywirusowego wraz z konsolą do zarządzania.”*** oznaczenie postępowania : DP.2301…….. 2019

Nawiązując do zamieszczonej w dniu …… na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 5 ustawy PZP oświadczamy, że:

nie należymy do tej samej grupy kapitałowej z żadnym z wykonawców, którzy złożyli ofertę w niniejszym postępowaniu *)

lub

należymy do tej samej grupy kapitałowej z następującymi Wykonawcami *)

w rozumieniu ustawy z dnia 16.02.2007r. o ochronie konkurencji i konsumentów.

Lista Wykonawców składających ofertę w niniejszy postępowaniu, należących do tej samej grupy kapitałowej *)

.....

.....

Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia

…… , dnia ……..…… r.

……..

Pieczątka i podpis/y osoby/osób uprawnionych

do składania oświadczeń woli w imieniu Wykonawcy

OPIS Przedmiotu zamówienia Załącznik nr 1 do SIWZ

Oprogramowanie antywirusowe wraz z konsolą do zarządzania.

I. Ilość licencji oprogramowania antywirusowego: **2200 szt**. gdzie co najmniej 25 % z tej puli można wykorzystać w ochronie systemów serwerowych.
II. Ważność licencji: **3 lata** od popisania umowy, ale nie wcześniej niż od **12.04.2019 r. ,kiedy wygasa licencja na poprzednie oprogramowanie antywirusowe.**
III. Jednodniowe szkolenie techniczne dla co najmniej 15 administratorów w siedzibie Zamawiającego.
IV. Instalacja systemu antywirusowego w siedzibie zamawiającego w terminie uzgodnionym z Zamawiającym.
V. Jednodniowa asysta inżyniera Wykonawcy w wdrożeniu oprogramowania antywirusowego wraz z wdrożeniem całego systemu zarządzania - uruchomienie konsoli zarządzającej oprogramowaniem antywirusowym.
VI. Asysta przy migracji do nowego systemu antywirusowego – co najmniej 8 godzin.
VII. Wsparcie techniczne : bezpłatna pomoc techniczna w okresie ważności licencji świadczona przez przeszkolonego inżyniera w języku polskim w dni robocze w godz. 8 -16.
VIII. Bezpłatna aktualizacja baz sygnatur wirusów oraz zakupionego oprogramowania w okresie ważności licencji.
IX. Ważność licencji od 12.04.2019 r. kiedy wygasa licencja na poprzednie oprogramowanie antywirusowe
X. Wykonawca udzieli 36 miesięcznej gwarancji, licząc od dnia podpisania bezusterkowego protokołu odbioru, na oprogramowanie

Oprogramowanie antywirusowe o minimalnych parametrach jak niżej:

1. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives

Ochrona antywirusowa i antyspyware

7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
9. Wbudowana technologia do ochrony przed rootkitami.
10. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
12. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
13. 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.
14. 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).
15. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
16. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
17. Możliwość skanowania dysków sieciowych i dysków przenośnych.
18. Skanowanie plików spakowanych i skompresowanych.
19. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
21. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
22. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
23. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
24. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
25. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
26. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
27. 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.
28. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).

29. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
30. 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).
31. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
32. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
33. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
34. 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.
35. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
36. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
37. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
38. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
39. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
40. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
41. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
42. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
43. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
44. 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.
45. 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.
46. 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 mają być

wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

47. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
48. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
49. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
50. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
51. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
52. 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.
53. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
54. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
55. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
56. 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.
57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
58. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
59. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
60. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
61. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
62. 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.

63. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
64. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
65. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
66. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
67. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - 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.
68. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
69. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
70. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
71. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
72. 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.
73. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
74. 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.
75. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
76. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.

77. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
78. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
79. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
80. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
81. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
82. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
83. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
84. 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.
85. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
86. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
87. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
88. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
89. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
90. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.
91. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP.
92. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
93. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
94. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.
95. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny
96. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

97. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.
98. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
99. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
100. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
101. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
102. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
103. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
104. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
105. Administrator ma możliwość dodania wykluczenia na podstawie procesu, wskazującego bezpośrednio na określony plik wykonywalny.
106. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania.
107. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.
108. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).
109. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”
110. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
111. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
112. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
113. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
114. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.

Ochrona przed spamem

115. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
116. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
117. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
118. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
119. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
120. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
121. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
122. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook.
123. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana".
124. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

125. Zapora osobista ma pracować jednym z 4 trybów:
    - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
    - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
    - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
    - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
126. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący.
127. Możliwość tworzenia list sieci zaufanych
128. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
129. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
130. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
131. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.

132. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
133. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
134. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
135. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
136. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
137. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
138. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
139. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
140. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
141. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.
142. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6
143. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
144. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
145. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o:
    - rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy.
    - rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP.

Kontrola dostępu do stron internetowych

146. Aplikacja musi być wyposażony w zintegrowany moduł kontroli odwiedzanych stron internetowych.
147. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
148. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
149. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
150. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
151. Podstawowe kategorie w jakie aplikacja musi być wyposażony to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol

i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
152. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
153. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
154. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
155. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
156. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2008 R2, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami i exploitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. 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).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
12. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
13. Możliwość skanowania dysków sieciowych i dysków przenośnych.
14. Skanowanie plików spakowanych i skompresowanych.
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
17. Aplikacja powinna wspierać mechanizm klastrowania.

18. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
19. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
20. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
21. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
22. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
23. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
24. 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.
25. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
26. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
27. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
28. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
29. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
30. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
31. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
32. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
33. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
34. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
35. 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.
36. 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.
37. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
38. Aktualizacje modułów analizy heurystycznej.
39. 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.

40. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
41. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
44. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
45. 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.
46. 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.
47. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
48. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
49. 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.
50. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
51. 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.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
53. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
54. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
55. 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.
56. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.

57. 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.
58. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
59. 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).
60. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
61. 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).
62. 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.
63. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
64. Aplikacja musi wspierać skanowanie magazynu Hyper-V
65. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
66. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki.
67. Administrator ma możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
68. Praca programu musi być niezauważalna dla użytkownika.
69. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
70. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
71. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”
72. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
73. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
74. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
75. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania.
76. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.
77. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).
78. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
79. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć

możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
80. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
81. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
82. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
83. Program musi posiadać system ochrony przed atakami sieciowymi (IDS).
84. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
85. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008 R2, 2012,2016 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych takich jak serwer Bazy danych, nazwę bazy danych, aktualny rozmiar bazy danych, nazwę hosta bazy danych
5. Serwer administracyjny musi oferować możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych
6. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
7. Rozwiązanie ma być w pełni zgodne z rozporządzeniem RODO
8. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
9. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
10. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
11. Konsola musi umożliwiać zarządzanie wszystkimi rozwiązaniami Producenta zabezpieczającymi przed zagrożeniami
12. Konsola musi umożliwiać zarządzanie systemem dynamicznej ochrony przed zagrożeniami
13. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
14. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
15. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
16. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.

17. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
18. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
19. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie „hardware fingerprint”
20. Serwer administracyjny musi oferować natywne wsparcie dla „VDI” oraz „Golden Master Image”
21. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
22. Instalacja serwera administracyjnego powinna oferować możliwość pracy w sieci rozproszonej nie wymagając dodatkowego serwera proxy.
23. Rozwiązanie ma oferować możliwość komunikacji agenta przy wykorzystaniu http Proxy wbudowanego w serwer centralnego zarządzania bez wykorzystania dodatkowej maszyny Proxy
24. Serwer musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
25. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
26. Serwer administracyjny musi oferować możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS
27. Serwer administracyjny musi oferować możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP
28. Serwer administracyjny musi oferować możliwość konfiguracji polityk zabezpieczeń takich jak ograniczenia funkcjonalności urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11
29. Serwer administracyjny musi oferować możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Map Google
30. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
31. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
32. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
33. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
34. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
35. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
36. Centralna administracja musi pozwalać na zarządzanie urządzeniami mobilnymi z systemem iOS
37. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
38. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

39. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
40. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
41. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów bazowych zarządzanego komputera oraz weryfikację zainstalowanego oprogramowania firm trzecich na stacji dla systemów Windows, Mac oraz Linux z możliwością jego odinstalowania
42. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
43. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
44. Konsola ma oferować możliwość aktywacji oraz wdrożenie elementów systemu EDR producenta.
45. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
46. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
47. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
48. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
49. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
50. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
51. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
52. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
53. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
54. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
55. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
56. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
57. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.

58. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
59. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
60. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
61. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
62. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
63. 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.
64. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
65. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
66. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
67. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
68. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
69. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
70. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
71. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
72. Serwer administracyjny musi oferować możliwość utworzenia grup dynamicznych na podstawie zainstalowanego oprogramowania oraz zainstalowanych podzespołów bazowych w komputerach końcowych.
73. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, podzespoły bazowe itp.
74. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
75. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
76. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
77. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na

stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.

78. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
79. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
80. Serwer administracyjny musi posiadać minimum 40 szablonów raportów przygotowanych przez producenta
81. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
82. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
83. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
84. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
85. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania oraz zapisania szablonów stworzonych filtrów
86. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
87. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
88. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
89. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie danych z systemu EDR producenta
90. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie informacje o zainstalowanych podzespołów w stacjach roboczych
91. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
92. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
93. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
94. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
95. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
96. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
97. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień na zasadzie „WYSIWYG” z wykorzystaniem istniejących zmiennych
98. Powiadomienia mailowe mają być wysyłane w formacie HTML
99. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.

100. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
101. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
102. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
103. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
104. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji bądź korzystając z powiązanego konta systemu zarządzania licencjami.
105. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
106. W przypadku posiadania tylko jednej dodanej licencji do konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania
107. Rozwiązanie ma oferować weryfikacji zainstalowanych komponentów bazowych urządzenia takich jak: 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, etc
108. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
109. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
110. Serwer administracyjny musi być wyposażony w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
111. W przypadku wystąpienia problemu rozwiązanie ma oferować możliwość przekierowania do wyszukiwarki Google z odwołaniem do konkretnego kodu błędu, który wystąpił w środowisku
112. Serwer administracyjny oferować łatwy dostęp do zadań z poziomu menu kontekstowego w zależności od rodzaju urządzenia.
113. Serwer administracyjny musi oferować aktualizację wszystkich komponentów z poziomu raportów jednym kliknięciem.
114. Serwer administracyjny musi oferować możliwość konfiguracji listy adresów multicast
115. Serwer administracyjny musi oferować WOL przy wykorzystaniu multicast
116. Rozwiązanie ma oferować instalację agenta rozwiązania DLP producenta z poziomu jednego repozytorium.
117. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.
118. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA.
119. Rozwiązanie ma oferować zebrania logu diagnostycznego którego pobranie będzie możliwe z poziomu konsoli WEB

120. Logi diagnostyczny, który można pobrać bezpośrednio z konsoli z modułów Anty SPM, firewall, HIPS, kontroli dostępu do urządzeń, kontroli dostępu do stron internetowych
121. Logi diagnostyczne do pobrania z poziomu konsoli mają być dostępne 24h od daty ich wygenerowania
122. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie
123. Konsola webowa musi umożliwiać weryfikację plików wysyłanych do serwerów producenta
124. Konsola webowa musi umożliwiać zarządzanie systemem EDR producenta.
125. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.
126. Konsola administracyjna musi oferować możliwość weryfikacji zmian w produktach wprowadzanych przez producenta (Release notes dostępne bezpośrednio z konsoli zarzadzania)
127. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar
128. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.
129. Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu interfejsu Konsoli administracyjnej
130. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.