SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)

Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie,
ul. Strzelecka 2, 31 – 503 Kraków

Przetarg nieograniczony pn.

„Dostawa oprogramowania antywirusowego”

Postępowanie będzie prowadzone z zastosowaniem przepisów
ustawy z dnia 29 stycznia 2004r.
Prawo zamówień publicznych (Dz.U.2017.1579 t.j. ze zm.)

o wartości szacunkowej poniżej kwot określonych w przepisach wydanych
na podstawie art. 11 ust. 8 PZP

Kraków, marzec 2018

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

„Dostawa oprogramowania antywirusowego"

1. **Zamawiający**:
   1.1. Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, 31-503 Kraków, ul. Strzelecka 2, NIP: 675-11-99-459, Fax: (12) 619-86-10, e-mail: zp@dzieciecyszpital.pl, www.dzieciecyszpital.pl
2. **Tryb udzielenia zamówienia:**
   2.1. Postępowanie prowadzone jest w trybie przetargu nieograniczonego zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U.2017.1579 t.j. ze zm.), zwanej w dalszej części SIWZ -PZP lub ustawą , a w sprawach nieuregulowanych przepisami PZP., ustawy z dnia 23 kwietnia 1964 r.- Kodeks cywilny (Dz.U.2017.459 j.t. ze zm.).
   2.2. Postępowanie prowadzone jest przez komisję przetargową powołaną do przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.
3. **Opis przedmiotu zamówienia**
   3.1. Przedmiotem zamówienia jest dostarczenie oprogramowania antywirusowego.
   3.2. Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1B do SIWZ.
   3.3. Nazwa i kod wg Wspólnego Słownika Zamówień (CPV): 48761000-0 Pakiety oprogramowania antywirusowego.
4. **Termin i sposób wykonania zamówienia.**
   4.1. Okres realizacji zamówienia do 14 dni od daty podpisania umowy.
   4.2. Szczegółowe warunki realizacji zamówienia określono w załączniku nr 2 do SIWZ (projekt umowy).
5. **Warunki udziału w postępowaniu oraz podstawy wykluczenia z postępowania. W postępowaniu o udzielenie zamówienia publicznego udział mogą brać wykonawcy, którzy:**
   5.1. Na podstawie art. 22 ust. 1 pkt 2) ustawy Prawo zamówień publicznych, Zamawiający nie określa warunków udziału w postępowaniu.
   5.2. Nie podlegają wykluczeniu z postępowania o udzielenie zamówienia publicznego z powodów określonych w art. 24 ust. 1 PZP.
6. **Wykaz oświadczeń lub dokumentów, potwierdzających spełnienie warunków udziału w postępowaniu oraz brak podstaw wykluczenia**
   6.1. Wykonawca dołącza do oferty aktualne na dzień składania ofert oświadczenie w zakresie wskazanym w załączniku nr 3a do SIWZ. Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu.
   6.2. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w pkt 6.1 powyżej składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to ma potwierdzać brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje brak podstaw wykluczenia.
   6.3. Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji z otwarcia ofert, o której mowa w art. 86 ust. 5 PZP, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 PZP. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Wzór oświadczenia będzie udostępniony przez Zamawiającego na stronie internetowej wraz z informacją z otwarcia ofert, o której mowa w art. 86 ust. 5 PZP.

6.4. Zamawiający przed udzieleniem zamówienia wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym - nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1, tj.:

6.4.1. Oświadczeń i dokumentów na potwierdzenie braku podstaw wykluczenia, o których mowa w art. 24 ust. 1 PZP.

6.4.1.1. Zamawiający nie będzie żądał od wykonawców przedłożenia oświadczeń i dokumentów na potwierdzenie braku podstaw wykluczenia wykonawcy, oprócz oświadczenia, o którym mowa w pkt 6.1 lub 6.2. SIWZ składanego przez wykonawcę wraz z ofertą.

6.5. Zgodnie z art. 24 aa PZP, Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu.

7. **Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami.**

7.1. Zamawiający dopuszcza, aby komunikacja między Zamawiającym a Wykonawcami odbywała się za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz.U.2017.1481 t.j. ze zm.), osobiście, za pośrednictwem posłańca, faksu lub przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną – pocztą elektroniczną.

7.2. Dane do korespondencji z Zamawiającym: pisemnie na adres Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, 31-503 Kraków, ul. Strzelecka 2, lub za pomocą faksu na numer: 12/ 619-86-68 lub drogą elektroniczną na adres e-mail: zp@dzieciecyszpital.pl.

7.3. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje za pośrednictwem faksu lub przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt ich otrzymania.

W przypadku wezwania przez Zamawiającego do złożenia, uzupełnienia lub poprawienia oświadczeń, dokumentów lub pełnomocnictw, w trybie art. 26 ust. 2 lub ust. 3 oraz ust. 3a PZP, oświadczenia, dokumenty lub pełnomocnictwa należy przedłożyć (złożyć/uzupełnić/ poprawić) w formie wskazanej przez Zamawiającego w wezwaniu.

7.4. Osobami uprawnionymi do kontaktu z wykonawcami są:
sprawy formalne: Marta Płatek, sprawy merytoryczne: Tadeusz Zamęta
fax. 12/619-86-68, e-mail: zp@dzieciecyszpital.pl.

8. **Wymagania dotyczące wadium.**

8.1. Zamawiający nie wymaga wniesienia wadium.

9. **Termin związania ofertą.**

9.1. Wykonawca pozostaje związany ofertą: **30** dni od ostatecznego terminu składania ofert. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

9.2. 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.

10. **Opis sposobu przygotowywania oferty.**

10.1. Oferta musi być podpisana przez osoby uprawnione do składania oświadczeń woli w imieniu Wykonawcy (wykonawców wspólnie ubiegających się o udzielenie zamówienia).

10.2. Ofertę należy złożyć pod rygorem nieważności w formie pisemnej. Zamawiający nie wyraża zgody na złożenie oferty w formie elektronicznej.

10.3. Wykonawca może złożyć tylko jedną ofertę, ponosząc koszty jej przygotowania i złożenia.

10.4. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu, z zastrzeżeniem treści art. 93 ust. 4 PZP.

10.5. Wszelkie podpisy winny być sporządzone w sposób umożliwiający ich identyfikację (np. wraz z imienną pieczątką osoby podpisującej), w celu możliwości jednoznacznej identyfikacji osoby podpisującej ofertę.

10.6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia w rozumieniu art. 23 ust. 1 ustawy.

10.6.1. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego (np. członkowie konsorcjum, przedsiębiorcy prowadzący działalność w formie spółki cywilnej) są zobowiązani ustanowić Pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i do zawarcia umowy.

10.6.2. Oprócz dokumentów wymienionych w pkt 6 SIWZ – wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego są zobowiązani do złożenia w ofercie Pełnomocnictwa ustanawiającego Pełnomocnika, o którym mowa w pkt 10.6.1.SIWZ. Pełnomocnictwo powinno być złożone w oryginale lub potwierdzonej notarialnie kopii i zawierać umocowanie do reprezentowania w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo, o którym mowa powyżej może wynikać albo z dokumentu pod taką samą nazwą, albo z umowy podmiotów składających wspólnie ofertę.

10.6.3. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, kopie dokumentów dotyczących odpowiednio wykonawcy są poświadczane za zgodność z oryginałem odpowiednio przez Pełnomocnika, o którym mowa w pkt. 10.6.1.

10.6.4. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego składają następujące dokumenty:

10.6.4.1. dotyczące każdego z wykonawców dokumenty wymienione w punkcie 6.1.,

10.6.4.2. pozostałe wymagane dokumenty winny być składane wspólnie.

10.7. Dokumenty wynikające z treści Rozporządzenia Prezesa Rady Ministrów z dnia 26 lipca 2016 roku w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz.U.2016.1126), składane w oryginale lub kopii poświadczonej za zgodność z oryginałem.

10.8. Poświadczenie za zgodność z oryginałem dokonuje odpowiednio wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.

10.9. Za osoby uprawnione uznaje się:

10.9.1. Osoby wskazane w dokumentach rejestrowych;

10.9.2. Osoby legitymujące się odpowiednim pełnomocnictwem udzielonym przez osoby, o których mowa w pkt. 10.6.1. Pełnomocnictwo należy dołączyć do oferty.

10.9.3. Osoby reprezentujące Wykonawców ubiegających się wspólnie o udzielenie zamówienia legitymujące się odpowiednim pełnomocnictwem dołączonym do oferty.

10.9.4. W przypadku, gdy ofertę składać będzie kilku przedsiębiorców prowadzących działalność w formie spółki cywilnej, a oferta nie będzie podpisana przez wszystkich wspólników, Wykonawca obowiązany jest dołączyć do oferty odpowiednie pełnomocnictwo udzielone przez pozostałych wspólników.

10.10. Treść złożonej oferty musi odpowiadać treści SIWZ.

10.11. Ofertę należy złożyć w zamkniętej kopercie, gwarantującej zachowanie poufności i jej nienaruszalność do terminu otwarcia ofert. Kopertę należy oznakować w niżej podany sposób:

a) nazwa i adres Wykonawcy,

b) adresat: Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31 – 503 Kraków, z napisem: **„Dostawa oprogramowania antywirusowego”,** znak sprawy: **DZP.271-5/18**, nie otwierać przed **04.04.2018r.** przed godziną 10.00.

10.12. Wszelkie poprawki (zmiany) w tekście oferty muszą być parafowane przez osoby podpisujące ofertę w sposób umożliwiający identyfikację osoby parafującej.

10.13. Wskazane jest, aby wszystkie kartki oferty były ponumerowane i spięte w sposób uniemożliwiający jej zdekompletowanie.

10.14. Zamawiający informuje: iż zgodnie 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 w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji (art. 11 ust. 4 Ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji - Dz. U. z 2018 r. poz. 419 j.t.). Wykonawca może zastrzec informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji. Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2018 r. poz. 419 j.t.) rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Nie później niż w terminie składania ofert wykonawca zobowiązany jest wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów wskazanych powyżej. Jeżeli wykonawca nie wykaże, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów wskazanych powyżej, nie będzie miał zastosowania zakaz wynikający z art. 8 ust. 3 PZP. Informacje zastrzeżone jako tajemnica przedsiębiorstwa powinny być przez Wykonawcę spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty i oznaczone napisem „informacje zastrzeżone".

10.15. Na zawartość oferty składa się:

10.15.1. wypełniony i podpisany Formularz ofertowy - zgodnie z załącznikiem nr 1A do SIWZ.

10.15.2. Stosowne Pełnomocnictwo (pełnomocnictwa) do reprezentowania wykonawcy w postępowaniu albo do reprezentowania wykonawcy w postępowaniu i zawarcia umowy, jeżeli osoba reprezentująca wykonawcę w postępowaniu o udzielenie zamówienia nie jest wskazana jako upoważniona do jego reprezentacji we właściwym rejestrze.

10.15.3. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument ustanawiający Pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie niniejszego zamówienia publicznego.

10.15.4. Wypełnione i podpisane oświadczenia, o którym mowa w pkt. w pkt 6.1 lub 6.2. SIWZ.

11. **Miejsce i termin składania i otwarcia ofert.**

11.1. Ofertę należy złożyć w terminie do **04.04.2018r** do godz. 9.30 w Biurze Dyrekcji Wojewódzkiego Specjalistycznego Szpitala Dziecięcego im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31 – 503 Kraków.

11.2. Otwarcie złożonych ofert nastąpi dnia **04.04.2018r** o godz. 10:00 w siedzibie Zamawiającego tj. w Sali Konferencyjnej przy ul. Strzeleckiej 2 w Krakowie.

11.3. Otwarcie ofert jest jawne.

11.4. Na podstawie art. 84 ust. 2 PZP., zamawiający niezwłocznie zwraca ofertę, która została wniesiona po terminie.

11.5. Wykonawca może, przed upływem terminu do składania ofert zmienić lub wycofać złożoną przez siebie ofertę pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian lub wycofaniu oferty przed upływem terminu składania ofert.

11.6. Powiadomienie o wprowadzeniu zmian lub wycofaniu oferty musi być oznaczone zgodnie z zapisem pkt. 10.11 SIWZ i dodatkowo opisane „Zmiana" lub „Wycofanie".

11.7. Wykonawca nie może wprowadzić jakichkolwiek zmian w treści złożonej oferty po upływie terminu składania ofert.

11.8. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę: jaką zamierza przeznaczyć na sfinansowanie zamówienia.

11.9. W trakcie otwierania kopert (paczek) z ofertami Zamawiający ogłosi obecnym:

11.9.1. kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia;

11.9.2. firmy oraz adresy wykonawców, którzy złożyli oferty w terminie;

11.9.3. ceny, termin wykonania zamówienia i warunki płatności zawarte w ofertach.

11.10. Niezwłocznie po otwarciu ofert zamawiający zamieszcza na stronie internetowej http://www.dzieciecyszpital.pl/szpital/przetargi-zamowienia-oferty/przetargi-2018.html informacje, o których mowa w pkt 11.9. SIWZ.

12. Opis sposobu obliczenia ceny (podatek VAT, winien być zgodny z obowiązującymi przepisami podatkowymi wg stawki na dzień składania ofert).

12.1. Wykonawca powinien wskazać cenę w załączniku nr 1A do SIWZ.

12.2. Cena oferty jest ceną ryczałtową brutto wskazaną w Formularzu ofertowym i obejmuje koszt wykonania całego przedmiotu zamówienia w zakresie określonym w pkt 3 SIWZ pn. „Opis przedmiotu zamówienia" oraz załączniku nr 1B do SIWZ.

12.3. Cena oferty musi być wyrażona w polskich złotych z dokładnością do drugiego miejsca po przecinku. Zamawiający nie będzie prowadził z Wykonawcą rozliczeń w walutach obcych.

12.4. Ponadto, w cenie oferty wykonawca winien również uwzględnić wszelkie koszty związane z realizacją przedmiotu zamówienia.

12.5. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując: nazwę (rodzaj) towaru, których dostawa będzie prowadzić do jego powstania oraz wskazując ich wartość bez kwoty podatku za dostawę objętą przedmiotem zamówienia - wskazanie niniejszego nastąpi w formularzu ofertowym. Brak wskazania powyższej informacji w treści załącznika nr 1A do SIWZ będzie jednoznaczny z brakiem powstania u Zamawiającego obowiązku podatkowego.

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

Lp.	KRYTERIUM:	WAGA
1	Cena	60 %
2	Termin dostawy	40 %
3	R a z e m	100 %

13.1. Sposób obliczania wartości punktowej ocenianego kryterium:

13.1.1. Kryterium 1 - Cena

$$\text{Najniższa cena brutto} = \frac{\text{najniższa cena oferowana wśród wszystkich podlegających ocenie ofert}}{\text{cena zaoferowana w badanej ofercie}} \times 60\ \%$$

13.1.2. Kryterium 2 – Termin dostawy

W kryterium „Termin dostawy" ocena zostanie dokonana w oparciu o informacje podane w formularzu ofertowym (załącznik nr 1A do specyfikacji) w następujący sposób. Jeżeli Wykonawca zaoferuje:

a) termin dostawy wynoszący do 14 – dni - otrzyma - 0 pkt,
b) termin dostawy wynoszący do 10 – dni otrzyma -20 pkt,
c) termin dostawy wynoszący do 7 – dni otrzyma - 40 pkt.

Zgodnie z powyższym opisem oferta z najkrótszym terminem dostawy tj. wynoszącym do 7 dni otrzyma największa ilość 40,00 punktów, oferta z terminem dostawy wynoszącym do 10 dni – 20,00 punktów oraz z terminem do 14 dni – 0,00 punktów.

Jeżeli wykonawca poda termin dostawy w niewłaściwy sposób, oferta wykonawcy podlegać będzie odrzuceniu na podstawie art. 89 ust. 1 pkt 2) PZP.

W przypadku braku skazania (nie wypełnienia) w pkt 3 formularza ofertowego terminu dostawy, Zamawiający przyjmie, że Wykonawca zaoferował termin dostawy wynoszący do 14 dni.

13.2. Przyjmuje się, że 1% = 1 pkt i tak zostanie przeliczona liczba uzyskanych punktów.

13.3. Jeżeli złożono ofertę, 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.

13.4. Maksymalna ilość możliwych do uzyskania punktów w ww. kryteriach, wynosi 100.

13.5. Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska najwyższą liczbę punktów wyliczoną jako sumę punktów uzyskanych w ww. kryteriach.

14. Informacje o formalnościach jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

14.1. O terminie i miejscu zawarcia umowy wykonawca, którego oferta została wybrana, jako najkorzystniejsza zostanie powiadomiony niezwłocznie po upływie terminu do wniesienia odwołania lub zakończeniu postępowania odwoławczego.

14.2. Jeżeli zostanie wybrana oferta Wykonawców wspólnie ubiegających się o zamówienie, Zamawiający będzie wymagał przed zawarciem umowy przedłożenia umowy regulującej współpracę tych Wykonawców.

14.3. Przed przystąpieniem do wykonania zamówienia wykonawca zobowiązany jest, o ile są już znane, podać nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w wykonanie przedmiotu umowy. Wykonawca zawiadamia Zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację przedmiotu umowy.

14.4. Brak przekazania przed podpisaniem, umowy, o której mowa w pkt. 14.2. będzie jednoznaczny z odmową podpisania umowy przez wykonawcę.

15. Zabezpieczenie należytego wykonania umowy.

15.1. Zamawiający nie żąda wniesienia zabezpieczenia należytego wykonania umowy.

16. Projekt umowy.

16.1. Projekt umowy stanowi załącznik nr 2 do SIWZ.

17. Pouczenie o środkach ochrony prawnej przysługującym wykonawcom w toku postępowania o udzielenie zamówienia.

17.1. Wykonawcom przysługują środki ochrony prawnej określone w Dziale VI PZP „Środki ochrony prawnej" (art. 179 - 198g PZP), tj. odwołanie do Prezesa Krajowej Izby Odwoławczej oraz skarga do sądu okręgowego właściwego dla siedziby Zamawiającego.

17.2. Środki ochrony prawnej (odwołanie oraz skarga) przysługują wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów PZP. Środki ochrony prawnej wobec Ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 PZP.

17.3. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami PZP czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie PZP. 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.

17.4. Odwołanie przysługuje wyłącznie wobec czynności:

17.4.1. określenia warunków udziału w postępowaniu,

17.4.2. wykluczenia odwołującego z postępowania o udzielenie zamówienia,

17.4.3. odrzucenia oferty odwołującego,

17.4.4. opisu przedmiotu zamówienia,

17.4.5. wyboru najkorzystniejszej oferty.

17.5. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej (02-676 Warszawa, ul. Postępu 17A) w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzono odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.

17.6. 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.

17.7. Odwołanie wnosi się w terminie 5 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia - jeżeli zostały przesłane w sposób określony w art. 180 ust. 5 zdanie drugie PZP (komunikacja elektroniczna) albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób.

17.8. Odwołanie wobec treści ogłoszenia o zamówieniu, a także wobec postanowień SIWZ wnosi się w terminie 5 dni od dnia publikacji ogłoszenia w Biuletynie Zamówień Publicznych lub zamieszczenia SIWZ na stronie internetowej.

17.9. Odwołanie wobec czynności innych niż określone w pkt 17.7 i 17. 8 SIWZ wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

17.10. Wykonawca może w terminie przewidzianym do wniesienia odwołania poinformować Zamawiającego o niezgodnej z przepisami PZP czynności podjętej przez niego lub zaniechaniu czynności, do której jest on zobowiązany na podstawie PZP, na które nie przysługuje odwołanie na podstawie art. 180 ust. 2 PZP.

17.11. Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu okręgowego właściwego dla siedziby Zamawiającego.

17.12. Skargę wnosi się za pośrednictwem Prezesa Krajowej Izby Odwoławczej w terminie 7 dni od dnia doręczenia orzeczenia Krajowej Izby Odwoławczej, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. Prawo Pocztowe (Dz.U. z 2017 r. poz. 1481 ze zm.) jest równoznaczne z jej wniesieniem.

17.13. Skarga powinna czynić zadość wymaganiom przewidzianym dla pisma procesowego oraz zawierać oznaczenie zaskarżonego orzeczenia, przytoczenie zarzutów, zwięzłe ich uzasadnienie, wskazanie dowodów, a także wniosek o uchylenie orzeczenia lub o zmianę orzeczenia w całości lub w części.

18. Pozostałe informacje:

18.1. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

18.2. Przewidywane zamówienia o których mowa w art. 67 ust. 1 pkt 6 i 7 PZP oraz okoliczności, po których zaistnieniu będą one udzielane.

18.2.1. Zamawiający nie przewiduje udzielenia zamówienia polegającego na powtórzeniu podobnych dostaw.

18.3. Opis sposobu przedstawiania ofert wariantowych oraz minimalne warunki jakim muszą odpowiadać oferty wariantowe wraz z wybranymi kryteriami oceny.

18.3.1. Zamawiający nie dopuszcza składania ofert wariantowych.

18.4. Adres poczty elektronicznej lub strony internetowej Zamawiającego.

18.4.1. Adres poczty elektronicznej: zp@dzieciecyszpital.pl,

18.4.2. Adres strony internetowej: www.dzieciecyszpital.pl

18.5. Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między zamawiającym a wykonawcą

18.5.1. Rozliczenia pomiędzy Zamawiającym a wykonawcą realizowane będą w złotych polskich (PLN).

18.6. Informacje dotyczące aukcji elektronicznej

18.6.1. Zamawiający nie przewiduje aukcji elektronicznej.

18.7. Wymagania, o których mowa w art. 29 ust. 3a PZP.

18.7.1. Nie dotyczy.

18.8. Wymagania, o których mowa w art. 29 ust. 4 pkt 1) PZP

18.8.1. Zamawiający nie określa wymagań, o których mowa w art. 29 ust. 4 pkt 1) PZP.

18.9. Informacje o obowiązku osobistego wykonania przez wykonawcę kluczowych części zamówienia

18.9.1. Zamawiający nie nakłada obowiązku osobistego wykonania kluczowych części zamówienia przez wykonawcę.

18.10. Standardy jakościowe, o których mowa w art. 91 ust. 2a PZP

18.10.1. Nie dotyczy

18.11. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

18.12. Procentowa wartość ostatniej części wynagrodzenia określona zgodnie z art. 143a ust. 3 PZP.

18.12.1. Nie dotyczy.

18.13. Zamawiający nie przewiduje ustanowienia dynamicznego systemu zakupów.

18.14. Zamawiający nie przewiduje zawarcia umowy ramowej.

18.15. Podwykonawstwo.

18.15.1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy/ podwykonawcom.

18.15.2. Zamawiający żąda wskazania przez wykonawcę w ofercie części zamówienia, której wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców.

18.15.3. Wskazanie niniejszego nastąpi w Formularzu ofertowym.

ZATWIERDZAM:

ZAŁĄCZNIKI DO SPECYFIKACJI:
Załącznik nr 1A – Formularz ofertowy
Załącznik nr 1B - Opis przedmiotu zamówienia
Załącznik nr 2 – Projekt umowy
Załączniki nr 3a – Oświadczenie z art. 25a ust. 1 PZP.

Załącznik nr 1A do SIWZ

.....
(miejscowość i data)

FORMULARZ OFERTOWY

W odpowiedzi na ogłoszenie o zamówieniu w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn. **„Dostawa oprogramowania antywirusowego”,** nr postępowania: DZP.271–5/18, zgodnie z wymaganiami określonymi w Specyfikacji Istotnych Warunków Zamówienia dla tego postępowania składamy niniejszą ofertę.

Dane dotyczące Wykonawcy

Nazwa.....

Siedziba.....

Nr telefonu /fax.....

E-mail .....

nr NIP..... nr REGON.....

Dane dotyczące Zamawiającego

Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków

1. Zobowiązuję się wykonać przedmiot zamówienia za ……. zł brutto, zgodnie z poniższą kalkulacja:

Cena jednostkowa brutto	**Ilość**	**Wartość brutto**	**Producent**	**Nazwa handlowa oferowanego oprogramowania**
…….	**258**	…….	…….	……

2. Oświadczam, że cena brutto podana w pkt 1 niniejszego formularza jest ceną ryczałtową i zawiera wszystkie koszty wykonania przedmiotu zamówienia, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.
3. **Przedmiot zamówienia zostanie zrealizowany w następującym terminie** (należy uzupełnić jeden wariant)**:**
   - **do 7 dni od daty podpisania umowy,**
   - **do 10 dni od daty podpisania umowy,**
   - **do 14 dni od daty podpisania umowy.**

4. Oświadczam, że jestem/nie jestem ** mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorcą.
5. Oświadczam, że wykonanie przedmiotu zamówienia nie spowoduje konieczności wykonania dodatkowych prac i nie będzie generowało dodatkowych kosztów Zamawiającego.

6. Oświadczam, że zapoznaliśmy się ze SIWZ (w tym z projektem umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w nim zawarte.
7. W przypadku udzielenia zamówienia, zobowiązuję się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego oraz na warunkach określonych w projekcie umowy stanowiącym załącznik nr 2 do SIWZ.
8. Oświadczam, że jestem związany niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.
9. Oferta wraz z załącznikami została złożona na ….. stronach.
10. Niniejszym oświadczamy, iż osobą/ami upoważnioną/ymi do reprezentacji Wykonawcy są.....
zgodnie z ..... /wpisać odpowiedni dokument/.
11. Niniejszym informuję, że informacje składające się na ofertę, zawarte na stronach ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji i jako takie nie mogą być ogólnie udostępnione***.
12. Podwykonawcom zamierzamy/ nie zamierzamy** powierzyć wykonanie następujących części zamówienia:
a/ wykonanie ..... oraz podajemy firmy (nazwę) podwykonawców realizujących wskazane części zamówienia ……***
W przypadku zatrudnienia podwykonawców odpowiadamy za ich pracę jak za swoją własną.
12. Do oferty załączamy następujące dokumenty:
1) ……
2) ……
13. Informuję/my, że dostawy dotyczące przedmiotu zamówienia będą prowadzić/ nie będą prowadzić (niepotrzebne skreślić) do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług. (W przypadku potwierdzenia, że dostawy dotyczące przedmiotu zamówienia będą prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, podana powyżej w pkt 1 cena jest ceną netto).**
14. Dane do umowy:

Osoby, które będą zawierały umowę ze strony Wykonawcy:		
Imię i nazwisko	Stanowisko	
Osoba(y) odpowiedzialna za realizację umowy ze strony Wykonawcy		
Imię i nazwisko	Stanowisko	Nr telefonu/ e-mail
Nr konta bankowego do rozliczeń pomiędzy Zamawiającym a Wykonawcą		
Nazwa i adres banku	Nr rachunku	

*** niepotrzebne skreślić*
****wypełnić jeśli dotyczy*

.....
(podpis i pieczęć osoby uprawnionej do reprezentacji Wykonawcy)

Załącznik nr 3a do SIWZ

.....
(pieczęć wykonawcy)

Oświadczenie wykonawcy
na podstawie art. 25a ust. 1 PZP

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dostawa oprogramowania antywirusowego”**, prowadzonego przez Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, oświadczam (-y), co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

1. Oświadczam (-y), że nie podlegam (-my) wykluczeniu z postępowania na podstawie art. 24 ust. 1 pkt 13-22 ZP.

…… *……*
Miejscowość, data *(podpis i pieczęć osoby uprawnionej do reprezentacji Wykonawcy)*

2. Oświadczam (-y), że zachodzą w stosunku do mnie (-nas) podstawy wykluczenia z postępowania na podstawie art. ……. PZP *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13 i 14, 16-20.* Jednocześnie oświadczam (-y), że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 PZP podjąłem (-liśmy) następujące środki naprawcze:
……
(należy wymienić wszystkie podjęte środki naprawcze w tym zakresie oraz przedstawić dowody na to, że podjęte środki są wystarczające do wykazania 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)

…… *……*
Miejscowość, data *(podpis i pieczęć osoby uprawnionej do reprezentacji Wykonawcy)*

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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

…… *……*
Miejscowość, data *(podpis i pieczęć osoby uprawnionej do reprezentacji Wykonawcy)*

Załącznik nr 2 do SIWZ

Umowa (projekt)

zawarta w Krakowie w dniu **……..**. pomiędzy:

Wojewódzkim Specjalistycznym Szpitalem Dziecięcym im. Św. Ludwika w Krakowie, 31-503 Kraków, ul. Strzelecka 2, zarejestrowanym w Sądzie Rejonowym dla Krakowa-Śródmieścia Wydział XI Gospodarczy Rejestrowy Krajowego Rejestru Sądowego pod nr KRS 0000009118, NIP 675-11-99-459, zwanym w dalszej części umowy „**Zamawiającym**" reprezentowanym przez:
Dyrektora – lek. med. Stanisława Stępniewskiego

a
……, NIP: ……., REGON: ……., zwanym w dalszej części umowy
„**Wykonawcą**", reprezentow1anym przez
…….

w rezultacie dokonania przez Zamawiającego wyboru Wykonawcy w trybie przetargu nieograniczonego zgodnie z Ustawą z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (Dz.U.2017.1579 t.j. ze zm.), - nr postępowania DZP.271-5/18, została zawarta umowa o następującej treści:

§1

1. Przedmiotem zamówienia jest dostarczenie i przeniesienie na własność Zamawiającego **oprogramowania**, zwanego dalej „przedmiotem umowy". Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1B do SIWZ/załącznik nr 1, które wraz z SIWZ i ofertą Wykonawcą stanowi integralną część niniejszej umowy.
2. Wykonawca zobowiązany jest zrealizować przedmiot umowy w terminie, o którym mowa w §2.
3. Przedmiot umowy przechodzi na własność Zamawiającego z chwilą potwierdzenia przez Zamawiającego odbioru i realizacji przedmiotu umowy

§2

Wykonawca zobowiązuje się zrealizować przedmiot umowy w **…….[1] dni od daty podpisania umowy.**

§ 3

1. Podstawą do wystawienia przez Wykonawcę faktury za cały należycie wykonany przedmiot umowy, o którym mowa w § 1 ust. 1 będzie potwierdzenie przez Zamawiającego odbioru i realizacji przedmiotu umowy.
2. Potwierdzenie, o którym mowa w ust. 1, winno zostać sporządzone niezwłocznie po zakończeniu realizacji przedmiotu umowy.

§ 4

[1] Zgodnie z deklaracja Wykonawcy w ofercie.

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za prawidłowo wykonany przedmiot umowy określony w § 1 ust. 1 wynagrodzenie ryczałtowe na kwotę **brutto: …….. zł** (słownie złotych: ……).
2. Kwota, o której mowa w ust. 1 obejmuje wszystkie koszty związane z realizacją przedmiotu umowy.

§ 5

1. Strony ustalają, że zapłata nastąpi w formie przelewu na rachunek bankowy Wykonawcy wykazany na fakturze w terminie **do 21 dni** od daty otrzymania prawidłowo wystawionej faktury przez Zamawiającego.
2. Ceny i nazwy na fakturze muszą odpowiadać cenom i nazwom ujętym w załączniku nr 1A (Formularz ofertowy) do umowy.
3. Datą zapłaty jest dzień obciążenia rachunku bankowego Zamawiającego.

§ 6

Strony ustalają, że osobami odpowiedzialnymi za realizację niniejszej umowy będą:
po stronie Wykonawcy – ……., tel. ……, e-mail: ……
po stronie Zamawiającego – Tadeusz Zamęta, tel. 12/ 619-86-76, e-mail: informatyka@dzieciecyszpital.pl

§ 7

1. W przypadku niewykonania lub nienależytego wykonania umowy przez Wykonawcę Zamawiający może obciążyć go karami umownymi w szczególności:
1) Wykonawca zobowiązuje się do zapłaty na rzecz Zamawiającego kary umownej w wysokości 10 % kwoty brutto, o której mowa w § 4 ust. 1 za odstąpienie od umowy przez Zamawiającego lub Wykonawcę z przyczyn leżących po stronie Wykonawcy.
2) Wykonawca zobowiązuje się do zapłaty na rzecz Zamawiającego kary umownej w wysokości 3 % wartości brutto umowy za każdy dzień opóźnienia w realizacji zobowiązania, o którym mowa w §1 ust. 1. W przypadku gdy kara umowna osiągnie wartość 15 % wynagrodzenia umownego brutto, o którym mowa w § 4 ust. 1 Zamawiający zastrzega sobie ponadto, prawo do rozwiązania umowy ze skutkiem natychmiastowym.
3) W pozostałych przypadkach w wysokości 5 % wartości brutto umowy.
4) Wykonawca wyraża zgodę na dokonanie przez Zamawiającego potrącenia naliczonych przez Zamawiającego kar umownych z należności Wykonawcy.
5) Naliczenie przez Zamawiającego bądź zapłata przez Wykonawcę kary umownej nie zwalnia go z zobowiązań wynikających z niniejszej umowy.
6) Wykonawca zastrzega sobie prawo do naliczania odsetek ustawowych w przypadku opóźnienia w stosunku do uzgodnionego terminu zapłaty.
7) W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonanej już części umowy.

§ 8

Wszelkie zmiany niniejszej umowy wymagają zgody obu Stron wyrażonej w formie pisemnej pod rygorem nieważności.

§ 9

Wykonawca nie może przenieść na osobę trzecią jakichkolwiek swoich wierzytelności wynikających z niniejszej umowy bez pisemnej zgody Zamawiającego, pod rygorem nieważności.

§ 10

W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy Ustawy Prawo zamówień publicznych oraz Kodeksu Cywilnego.

§ 11

1. Strony zobowiązują się do polubownego rozwiązywania wszelkich sporów mogących powstać na tle wykonywania niniejszej umowy.
2. Ewentualne spory wynikłe w trakcie realizacji umowy będą załatwiane polubownie, a w przypadku braku porozumienia rozstrzygającym spór jest Sąd powszechny właściwy dla siedziby Zamawiającego.

§ 12

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

WYKONAWCA **ZAMAWIAJĄCY**

Załącznik nr 1B do SIWZ

ESET Endpoint Security Suite kontynuacja - 258 stacji końcowych (klucz licencyjny) zawierający: (Ochrona przed szkodliwym oprogramowaniem dla stacji roboczych, Ochrona przed szkodliwymi programami dla serwerów plików (możliwość instalacji dla min. 30% licencji), Ochrona i zarządzanie urządzeniami mobilnymi, Kontrola (aplikacji, urządzeń, sieci), Konsola zarządzająca) lub równoważny**
W załączniku nr 1A do SIWZ (Formularz ofertowy) wymagane jest podanie producenta oraz nazwy handlowej oferowanego oprogramowania.

** za równoważny Zamawiający uzna oprogramowanie spełniające standardy jakościowe systemu wymagane przez Zamawiającego oraz współpracujące bez zakłóceń z systemami operacyjnymi stacji roboczych (Microsoft Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 10) i serwerów (Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016) posiadanymi przez Zamawiającego. W przypadku zaoferowania systemu równoważnego Zamawiający wymaga zainstalowania i skonfigurowania dostarczonego oprogramowania na wskazanych serwerach i stacjach roboczych zabezpieczanych dotychczas przez oprogramowanie ESET (w tym odinstalowania działającego na tych stacjach oprogramowania ESET). Skonfigurowania zaoferowanego oprogramowania (utworzenie odpowiednich grup komputerów, przypisanie komputerów do poszczególnych grup, zdefiniowania odpowiednich reguł aktualizacji, skanowania. Firewall dla poszczególnych grup komputerów i konsoli zarządzającej zgodnie z wymaganiami Zamawiającego). Przeszkolenia administratorów Zamawiającego 3 osoby z administracji, konfiguracji i instalacji wdrożonego oprogramowania (min. 2 dni po 3 godz. szkolenia). Instalacja i konfiguracja ma przebiegać w sposób nie zakłócający pracy użytkowników, stacji roboczych oraz serwerów.
Opis wymagań dostarczanego systemu:

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 10
2. Wersja programu dla stacji roboczych Windows dostępna co najmniej w języku polskim.

Ochrona antywirusowa i antyspyware

3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wbudowana technologia do ochrony przed rootkitami.
5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. 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.
8. 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
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
11. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
12. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
13. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
14. 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.
15. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).

16. 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).
17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
20. 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.
21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
28. 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.
29. 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.
30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
32. 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.
33. 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.
34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
35. 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.

36. 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.
37. 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.
38. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
39. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
40. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
41. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
42. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
43. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
44. 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.
45. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
46. 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.
47. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
48. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
50. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
51. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
52. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
53. 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.
54. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
55. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
56. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
57. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.

Ochrona przed spamem

58. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.

59. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
60. 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.
61. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
62. 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.
63. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
64. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
65. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook.
66. 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".
67. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

68. 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.
69. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący
70. Możliwość tworzenia list sieci zaufanych.
71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
72. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
73. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
78. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
80. 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.

81. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.

Kontrola dostępu do stron internetowych

83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
84. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
86. Podstawowe kategorie w jakie aplikacja musi być wyposażona 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.
87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
89. 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 2003, 2008, 2008 R2, 2012, 2012 R2, 2016
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. 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.
13. Aplikacja powinna wspierać mechanizm klastrowania.
14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
18. 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.

19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
27. 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.
28. 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.
29. 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.
30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
31. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
32. 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.
33. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
34. 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.
35. 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.
36. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
37. 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.
38. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
39. 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.
40. 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).
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Aplikacja musi wspierać skanowanie magazynu Hyper-V
43. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów

44. 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).
45. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
46. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012
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. 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.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający co najmniej polski i angielski..
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
12. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
13. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
14. 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.
15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
16. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
17. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
18. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
19. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
20. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
21. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
22. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.

23. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
24. 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.
25. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
26. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
27. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
28. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
29. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
30. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
31. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
32. 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.
33. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
34. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
35. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
36. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
37. 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, itp.
38. 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.
39. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
40. 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.
41. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
42. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
43. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
44. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
45. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
46. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.

47. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
48. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
49. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
50. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
51. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
52. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
53. 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.