**Oferta na:**

# Zakup Oprogramowania antywirusowego

**Numer ogłoszenia IW.0401.002.2022**

**Data zamieszczenia: 08.02.2022**

## Zamawiający :

## Krakowski Szpital Specjalistyczny im. Jana Pawła II,

## ul. Prądnicka 80, 31-202 Kraków

## A. Informacie dotyczące zamówienia;

1) Miejsce składania ofert:

- Ofertę opatrzoną pieczęcią Wykonawcy należy złożyć w siedzibie Zamawiającego przy ul. Prądnickiej **80** w Krakowie w budynku Administracyjno-Konferencyjnym - Pawilon A-V (Dziennik Podawczy) do dnia **22.02.2021**, do godziny **9:00.** Oferty złożone po terminie nie będą otwierane i zostaną niezwłocznie zwrócone Wykonawcy.

2) Prowadzone postępowanie nie stanowi przetargu w rozumieniu Kodeksu cywilnego ani ustawy Prawo Zamówień Publicznych. Zamawiający nie jest zobligowany do wyboru jakiejkolwiek oferty, a złożenie oferty nie stanowi podstawy do występowania z jakimikolwiek roszczeniami wobec Zamawiającego ze strony podmiotu, który złożył ofertę.

3) Warunki zgłaszania ofert:

- Wykonawca musi posiadać uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.
    - Wykonawca posiada wiedzę i doświadczenie odpowiednie do wykonania zamówienia.
    - Wykonawca może zaproponować tylko jedną cenę i nie może jej zmienić,
    - Oferta zawiera datę końcową związania ofertą, nie krótszą niż 3 tygodnie od daty złożenia oferty,

- Ofertę składa się pod rygorem nieważności w formie pisemnej, w zamkniętej kopercie lub innym opakowaniu, wyraźnie oznaczonej numerem postępowania wskazanym w zaproszeniu lub na platformie zakupowej szpitala.

## Ogłoszenie na:

## Oferta na: Zakup Oprogramowania antywirusowego

## Numer ogłoszenia IW.0401.002.2022

Zamawiający nie dokonuje wyboru ofert, jeżeli:

a)oferta z najkorzystniejszą ceną przekracza kwotę, którą zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,

b}wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonania zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć

4) Oferta wraz z załącznikami musi być podpisana przez osobę/osoby uprawnione do składania oświadczeń woli w imieniu wykonawcy zgodnie z zasadami reprezentacji. Jeżeli osoba/ osoby podpisująca ofertę działa na podstawie pełnomocnictwa, to pełnomocnictwo to musi w swej treści jednoznacznie wskazywać uprawnienie do podpisania oferty. Pełnomocnictwo to musi być dołączone do oferty i musi być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez osobę wymienioną w rejestrze, która jest wskazana, jako upoważniona do reprezentowania Wykonawcy lub przez notariusza.

5) Oferta musi być sporządzona w języku polskim. Każdy dokument składający się na ofertę sporządzony w innym języku niż język polski powinien być złożony wraz z tłumaczeniem na język polski.

## B. Wymagania wobec Wykonawców:

1) Zamówienie dotyczy dostarczenia oprogramowania antywirusowego wraz z konsolą zarządzającą oraz pełnego wdrożenia systemu wraz z przeprowadzeniem warsztatów wdrożeniowych z funkcjonalności systemu antywirusowego
2) Wykonawca, przed złożeniem oferty, ma prawo zapoznać się z istniejącą infrastrukturą i warunkami technicznymi w Szpitalu KSS im. Jana Pawła II.
3) Wykonawca zapewni jednodniowe szkolenie wdrożeniowe związane z administracją wdrożonego systemu
4) Wykonawca musi w ofercie wskazać konkretne typy proponowanych produktów (nazwa oprogramowania, licencji)
5) Wykonawca musi przedstawić w ofercie, minimum dwie referencje w zakresie przeprowadzonych wdrożeń proponowanego systemu

## A. Wymagania ogólne:

1) Wykonawca jest zobowiązany do dostarczenia licencji:
   a. na oferowany system antywirusowy – 85 licencji na stacje robocze minimum na 3 lata
   b. na oferowany serwer zarządzający – 1 licencja minimum na 3 lata
2) Wdrożenia serwera zarządzającego systemu antywirusowego w oparciu o serwer fizyczny dostarczony przez Wykonawcę lub serwer zainstalowany w środowisku wirtualnym Zamawiającego (platforma VMWare) , w oparciu o dostarczone licencje na OS.
3) Wdrożenia systemu antywirusowego na stacjach roboczych i serwerach, w siedzibie Zamawiającego, polegającego na usunięciu aktualnie użytkowanego systemu antywirusowego i zainstalowaniu proponowanego rozwiązania.
4) Przeprowadzenia szkolenia wdrożeniowego obejmującego funkcjonalności oferowanego systemu antywirusowego.
5) Wykonawca zobowiązuje się do wykonania wszelkich prac z zachowaniem najwyższej staranności
6) W celu ograniczenia kosztów Wykonawca może wykorzystać posiadany już przez zamawiającego serwer zarządzający Kaspersky Security Center 11

## B. Warunki gwarancji i wsparcia dla oprogramowania, wdrożenia:

1) Na dostarczaną usługę musi być udzielona min. 36 miesięczne wsparcie od daty zakończenia wdrożenia, oparta o świadczenie gwarancyjne producenta oprogramowania, niezależnie od statusu partnerskiego wykonawcy; serwis gwarancyjny świadczony ma być w miejscu instalacji oprogramowania.
2) Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań. Zamawiający wymaga zdefiniowania procedury zgłaszania awarii, w tym: numerów telefonów, faksów, adresów e-mail oraz wymaganych formularzy.

3) Oprogramowanie musi zostać zainstalowane na 100% stacji i serwerów wskazanych przez Zamawiającego.
4) Wdrożenie musi obejmować zaaplikowanie grup, zadań i polityk bezpieczeństwa identycznych z aktualnie użytkowanymi przez Zamawiającego.

## C. Terminy wykonania:

1) Całkowite wykonanie Zamówienia przez Wykonawcę nastąpi nie później niż maksimum 3 dni od daty zawarcia umowy.

## D. Wymagania techniczne dla ochrony stacji:

1) Program musi wspierać następujące platformy:
    a. Microsoft Windows 10 Enterprise x86 Edition
    b. Microsoft Windows 10 Enterprise x64 Edition
    c. Microsoft Windows 8.1 Enterprise x86 Edition
    d. Microsoft Windows 8.1 Enterprise x64 Edition
    e. Microsoft Windows 8 Professional / Enterprise x86 Edition
    f. Microsoft Windows 8 Professional / Enterprise x64 Edition
    g. Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition
    h. Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition
    i. Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP
    j. Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
    k. Microsoft Windows Vista® x86 Edition SP2
    l. Microsoft Windows Vista x64 Edition SP2
    m. Microsoft Windows XP Professional x86 Edition SP3
2) Program musi obsługiwać minimalne konfiguracje sprzętowe:
    a. Dla systemu Microsoft Windows XP Professional x86 Edition SP3: procesor Intel Pentium 1 GHz lub równoważny, 512 MB wolnej pamięci RAM
    b. Dla systemów 32-bitowych Windows Vista oraz nowszych: procesor Intel Pentium 1 GHz lub równoważny, 1 GB wolnej pamięci RAM
    c. Dla systemów 64-bitowych Windows Vista oraz nowszych: Intel Pentium 2 GHz lub równoważny, 1 GB wolnej pamięci RAM
3) System musi posiadać polskojęzyczny interfejs konsoli zarządzającej i programu na stacjach roboczych i serwerach.
4) Program musi posiadać certyfikaty niezależnych laboratoriów.
5) Program musi zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
6) Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
7) Program musi posiadać możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury.

8) Program musi posiadać możliwość wyświetlenia podsumowania o aktywności, reputacji i lukach w aplikacjach aktualnie uruchomionych w systemie.
9) Program musi posiadać możliwość monitorowania prób uruchamiania aplikacji przez użytkowników zgodnie z określonymi regułami.
10) Program musi posiadać możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.
11) Program musi posiadać dedykowany moduł blokujący określone kategorie urządzeń (np. pamięci masowe, urządzenia Bluetooth itp.).
12) Program musi posiadać możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik, określenia przedziału czasu, w którym użytkownik będzie miał możliwość tylko zapisu bądź tylko odczytu, ewentualnie zapisu i odczytu.
13) Program musi posiadać możliwość blokowania urządzeń według ich rodzaju: dyski, USB, drukarki itp. w zależności od czasu, konta użytkownika systemu Windows oraz rodzaju operacji: odczyt/zapis.
14) Program musi posiadać możliwość utworzenia listy zaufanych urządzeń na podstawie modelu, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.
15) Program musi posiadać możliwość kontroli dostępu do zasobów sieciowych w zależności od ich zawartości i lokalizacji:
    a. Możliwość definiowania reguł filtrujących zawartość na wybranej stronie lub wszystkich stronach w zależności od kategorii zawartości: pornografia, narkotyki, broń, gry, sieci społecznościowe, banery, itd.
    b. Możliwość definiowania reguł blokujących bądź zezwalających na wyświetlanie określonej treści na wybranej stronie lub wszystkich stronach w zależności od kategorii danych: pliki wideo, audio, archiwa itd.
16) Program musi posiadać monitor wykrywania luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.
17) Program musi posiadać możliwość ochrony przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX).
18) Program musi posiadać możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
19) Program musi posiadać wbudowany moduł skanujący protokoły POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.
20) Skaner poczty musi mieć możliwość zmiany nazwy lub usuwania określonych typów załączników.
21) Program musi posiadać wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.
22) Program musi posiadać wbudowany moduł skanujący ruch komunikatorów ICQ, MSN, AIM, Mail.Ru Agent oraz IRC.
23) Program musi posiadać wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
24) Program musi posiadać możliwość określenia poziomu czułości modułu heurystycznego.
25) Program musi posiadać wbudowany moduł skanujący skrypty napisane w językach VB Script i Java Script wykonywane przez system operacyjny Windows oraz program Internet Explorer.
26) Program musi posiadać wbudowany moduł kontrolujący dostęp do rejestru systemowego.
27) Program musi posiadać wbudowany moduł kontrolujący dostęp do ustawień Internet Explorera.

28) Program musi posiadać wbudowany moduł chroniący przed phishingiem.

29) Program musi posiadać moduł zapory ogniowej z możliwością:

    a. Tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji.

    b. Tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP.

    c. Zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.

30) Program musi posiadać możliwość ochrony przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów.

31) Program musi posiadać możliwość kontroli systemu poprzez ochronę proaktywną przed nowymi zagrożeniami, które nie znajdują się w antywirusowych bazach danych:

    a. Kontrola aktywności aplikacji, dostarczanie szczegółowych informacji dla innych modułów aplikacji w celu zapewnienia jeszcze bardziej efektywnej ochrony.

    b. Możliwość wycofywania zmian wprowadzanych w systemie przez szkodliwe oprogramowanie nawet w poprzednich sesjach logowania.

32) Program musi posiadać możliwość centralnego zbierania i przetwarzanie alarmów w czasie rzeczywistym.

33) Program musi posiadać możliwość leczenia i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.

34) Program musi posiadać możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.

35) Program musi posiadać terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.

36) Program musi posiadać możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.

37) Program musi posiadać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.

38) Program musi posiadać możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych, dostęp do rejestru oraz ruch sieciowy.

39) Program musi posiadać możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.

40) Program musi posiadać funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.

41) Program musi posiadać możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.

42) Program musi posiadać możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.

43) Program musi posiadać możliwość zablokowania hasłem operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu.

44) Program musi posiadać możliwość zdefiniowania portów, które będą monitorowane lub wykluczone z monitorowania przez moduły skanujące ruch sieciowy (z wyłączeniem zapory ogniowej).

45) Program musi posiadać możliwość skanowania w czasie rzeczywistym:

a. Uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików.
b. Pobieranej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP i NNTP niezależnie od klienta pocztowego.
c. Plików pobieranych z Internetu po protokole HTTP.
d. Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego.
e. Treści i plików przesyłanych z wykorzystaniem komunikatorów ICQ, MSN, AIM, Mail.Ru Agent oraz IRC.

46) W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:
a. Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt
b. Rejestrować w pliku raportu informację o wykryciu wirusa
c. Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND
d. Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku
e. Poddać kwarantannie podejrzany obiekt

47) Skaner antywirusowy musi posiadać możliwość uruchamiania automatycznie zgodnie z terminarzem i skanowania wszystkich lokalnych dysków twardych komputera.

48) Program musi posiadać możliwość informowania o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania.

49) System antywirusowy musi posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.

50) Program musi posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.

51) Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.

52) Program musi posiadać możliwość określenia źródła uaktualnień.

53) Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw uaktualnień po zakończeniu aktualizacji.

54) Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.

55) Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.

56) Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.

57) Program musi posiadać możliwość pobierania uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).

58) Program musi posiadać możliwość raportowania zdarzeń informacyjnych.

59) Program musi posiadać możliwość określenia okresu przechowywania raportów.

60) Program musi posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.

61) Program musi posiadać możliwość wyłączenia zaplanowanych zadań skanowania podczas pracy na bateriach.

62) Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.

## E. Wymagania techniczne dla ochrony serwerów:

1) Program musi wspierać następujące platformy:
    a. Microsoft Small Business Server 2011 Standard x64
    b. Microsoft Windows Server 2012 R2 Standard x64
    c. Microsoft Windows Server 2012 Foundation / Standard x64
    d. Microsoft Windows Server 2008 R2 Standard x64
    e. Microsoft Windows Server 2008 R2 Standard x64 SP1
    f. Microsoft Windows Server 2008 R2 Enterprise x64
    g. Microsoft Windows Server 2008 R2 Enterprise x64 SP1
    h. Microsoft Windows Server 2008 Standard x86 / x64 SP2
    i. Microsoft Windows Server 2008 Enterprise x86 / x64 SP2
    j. Microsoft Windows Server 2003 R2 Standard x86 / x64 SP2
    k. Microsoft Windows Server 2003 R2 Enterprise x86 / x64 SP2
    l. Microsoft Windows Server 2003 Standard x86 / x64 SP2
    m. Microsoft Windows Server 2003 Enterprise x86 / x64 SP2
2) Program musi obsługiwać minimalne konfiguracje sprzętowe:1 GB pamięci RAM, Intel Pentium 1 GHz lub równoważny
3) Program musi posiadać polskojęzyczny interfejs konsoli programu i jego monitora na serwerach plików.
4) Program musi posiadać certyfikaty niezależnych laboratoriów.
5) Program musi zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
6) Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
7) Program musi mieć możliwość ochrony w czasie rzeczywistym
8) Program ma możliwość skanowania i klasyfikowania plików na podstawie informacji gromadzonych w oparciu o technologię chmury.
9) Program musi mieć możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.
10) Program musi zapewniać ochronę przed wszystkimi typami wirusów, robaków i koni trojańskich, a także złośliwym kodem.
11) Program musi posiadać możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
12) Program musi posiadać wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
13) Program musi posiadać możliwość określenia poziomu czułości modułu heurystycznego.
14) Program musi posiadać moduł zapory ogniowej z możliwością:
    a. Tworzenia reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji, w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji.
    b. Tworzenia nowych zestawów warunków i działań wykonywanych na pakietach sieciowych

oraz strumieniach danych dla określonych protokołów, portów i adresów IP.

c. Zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.

15) Program musi zapewniać ochronę przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów.
16) Program musi umożliwiać centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
17) Program musi umożliwiać leczenie i usuwanie plików z archiwów następujących formatów RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
18) Program musi posiadać możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.
19) Program musi posiadać wbudowany terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
20) Program musi posiadać możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.
21) Program musi posiadać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
22) Program musi posiadać możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność plikowa, aktywność aplikacji, nie będą dziedziczone ograniczenia nadrzędnego procesu, nie będzie monitorowana aktywność aplikacji potomnych.
23) Program musi posiadać możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
24) Program musi posiadać możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.
25) Program musi posiadać możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
26) Program musi posiadać możliwość zablokowania hasłem operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu.
27) W przypadku wykrycia wirusa monitor antywirusowy program musi automatycznie:
    a. Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt
    b. Rejestrować w pliku raportu informację o wykryciu wirusa
    c. Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND
    d. Utworzyć kopie zapasową przed podjęciem próby leczenia lub usunięcia zainfekowanego pliku
    e. Poddać kwarantannie podejrzany obiekt
28) Skaner antywirusowy musi posiadać możliwość uruchamiania automatycznie zgodnie z terminarzem; możliwość skanowania wszystkich lokalnych dysków komputera.
29) System antywirusowy musi posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
30) Program musi posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
31) Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
32) Program musi posiadać możliwość określenia źródła uaktualnień.
33) Program musi posiadać możliwość określenia katalogu, do którego będzie kopiowany zestaw

uaktualnień po zakończeniu aktualizacji.

34) Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.
35) Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
36) Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
37) Antywirusowe bazy danych na serwerach producenta musza być aktualizowane nie rzadziej niż raz na godzinę.
38) Program musi posiadać możliwość pobierania uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).
39) Program musi posiadać możliwość raportowania zdarzeń informacyjnych.
40) Program musi posiadać możliwość określenia okresu przechowywania raportów.
41) Program musi posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych oraz kwarantannie.
42) Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.

## F. Wymagania techniczne dla serwera zarządzania:

1) System scentralizowanego zarządzania musi obsługiwać następujące systemy operacyjne:
    a. Microsoft Windows XP Professional SP3
    b. Microsoft Windows XP Professional x64 SP3
    c. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 i wyższy (x32/x64)
    d. Microsoft Windows 7 Professional/Enterprise/Ultimate (x32/x64)
    e. Microsoft Windows 8 Professional / Enterprise (x32/x64)
    f. Microsoft Windows 8.1 Professional / Enterprise (x32/x64)
    g. Microsoft Windows 10 Professional / Enterprise (x32/x64)
    h. Microsoft Windows 10 Professional / Enterprise (x32/x64)
    i. Microsoft Windows Server 2003 SP2 (wszystkie edycje)
    j. Microsoft Windows Server 2003 x64 SP2 (wszystkie edycje)
    k. Microsoft Windows Server 2008 (wszystkie edycje)
    l. Microsoft Windows Server 2008 x64 (wszystkie edycje)
    m. Microsoft Windows Server 2008 x64 SP1 (wszystkie edycje)
    n. Microsoft Windows Server 2008 R2 (wszystkie edycje)
    o. Microsoft Windows Server 2012 (wszystkie edycje)
    p. Microsoft Windows Server 2012 R2 (wszystkie edycje)
    q. Microsoft Windows Small Business Server 2003 SP2 (wszystkie edycje)
    r. Microsoft Windows Small Business Server 2008 (wszystkie edycje)

s. Microsoft Windows Small Business Server 2011 (wszystkie edycje)

2) System zdalnego zarządzania musi posiadać polskojęzyczny interfejs konsoli programu.
3) System zdalnego zarządzania musi umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory).
4) System zdalnego zarządzania musi umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły.
5) System zdalnego zarządzania musi umożliwiać ograniczenie pasma sieciowego wykorzystywanego do komunikacji stacji z serwerem administracyjnych. Reguły musza umożliwić ograniczenia w oparciu o zakresy adresów IP oraz przedziały czasowe.
6) System zdalnego zarządzania musi umożliwiać tworzenie hierarchicznej struktury serwerów administracyjnych jak również tworzenie wirtualnych serwerów administracyjnych.
7) System zdalnego zarządzania musi umożliwiać zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.
8) Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych musi być szyfrowana przy użyciu protokołu SSL.
9) Konsola administracyjna musi posiadać możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych Zamawiającego.
10) Zarządzanie aplikacjami musi się odbywać przy użyciu profili aplikacji oraz zadań.
11) Konsola administracyjna musi mieć możliwość informowania administratorów o wykryciu epidemii wirusa.
12) Serwer zarządzający musi mieć możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).
13) System centralnego zarządzania musi być wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych.
14) System musi mieć możliwość centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.
15) System musi mieć możliwość centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania.
16) System musi mieć możliwość centralnego zbierania informacji i tworzenia sumarycznych raportów.
17) System zdalnego zarządzania musi umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formatach HTML, XML i PDF).
18) System zdalnego zarządzania musi umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.
19) System zdalnego zarządzania musi umożliwiać tworzenie kategorii aplikacji i warunków ich uruchomienia.
20) System zdalnego zarządzania musi umożliwiać przeglądanie informacji o aplikacjach i plikach wykonywalnych znajdujących się na stacjach roboczych.
21) Program musi mieć możliwość dezinstalacji aplikacji niekompatybilnych jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika.
22) System zdalnego zarządzania musi wyświetlać szczegółowe informacje na temat luk w

oprogramowaniu wykrytych na zarządzanych komputerach

23) System zdalnego zarządzania musi mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.

24) System zdalnego zarządzania musi umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie).

25) System zdalnego zarządzania musi umożliwiać przeglądanie informacji o kopiach zapasowych obiektów wyleczonych/usuniętych na stacjach roboczych wraz z możliwością ich przywrócenia do początkowej lokalizacji i/lub zapisania na stacji administratora.

26) System zdalnego zarządzania musi umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania.

27) System zdalnego zarządzania musi umożliwiać automatyczne instalowanie licencji na stacjach roboczych.

28) System zdalnego zarządzania musi umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania.

29) System zdalnego zarządzania musi umożliwiać automatyczne uruchomienie wyłączonych komputerów przed wykonaniem odpowiednich zadań administracyjnych (z wykorzystaniem funkcji Wake-On-LAN) a po zakończeniu wykonywania zadań ich wyłączenie. Funkcjonalność ta nie może być ograniczona tylko do podsieci, w której znajduje się serwer administracyjny.

30) System zdalnego zarządzania musi umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści.

31) System zdalnego zarządzania musi umożliwiać zdalne włączanie, wyłączanie oraz restartowanie komputerów wraz z możliwością interakcji z użytkownikiem (np. natychmiastowe wykonanie działania lub jego odłożenie na zdefiniowany okres czasu).

32) Program musi umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji, ikony w pasku systemowym, wpisów w Menu Start oraz na liście zainstalowanych programów.

33) Program musi umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.

34) System zdalnego zarządzania musi mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.

35) System zdalnego zarządzania musi tworzyć listę kont użytkowników sieci. Do tworzenia powinny być wykorzystywane różne źródła w tym min. AD, kontrolery domen oraz lokalne konta na komputerach.

36) System zdalnego zarządzania musi umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu poczty elektronicznej lub wiadomości SMS.

37) W całym okresie trwania subskrypcji użytkownik musi mieć prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.

38) W całym okresie trwania subskrypcji użytkownik musi mieć możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej.