SAMODZIELNY PUBLICZNY
ZAKŁAD OPIEKI ZDROWOTNEJ
w WIELUNIU
98-300 Wieluń
ul. Szpitalna 16

**Nr sprawy: SPZOZ-OiZP/2/24/241/ 30 – 19/ A /2016** Wieluń, dn. 31.10.2016 r.

**OGŁOSZENIE O ZAMÓWIENIU DO 30 tys. EURO**

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Wieluniu, ul. Szpitalna 16 ogłasza postępowanie w sprawie wydatkowania środków publicznych - na podstawie art. 4 ust 8 Ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych (Zamówienie poniżej 30 tys. euro – nie stosuje się przepisów ustawy Pzp) oraz na podstawie Regulaminu Postępowania przy Udzielaniu Zamówień Publicznych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Wieluniu wprowadzonego Zarządzeniem Dyrektora SPZOZ w Wieluniu nr 01/010/9/2016 z dnia 20.05.2016 r. ( pkt 2 ppkt 2.4 w trybie: Zaproszenie do składania ofert).

**SPZOZ w Wieluniu zaprasza Wykonawców do składania ofert - propozycji cenowych na:**

**„Przedłużenie licencji na program antywirusowy ESET EndPoint Antywirus– szt. 60 i zakup dodatkowych licencji na program antywirusowy ESET EndPoint Antywirus – szt. 60."**

**I. Opis przedmiotu zamówienia:**

1. Przedmiotem zamówienia jest przedłużenie licencji na program antywirusowy ESET EndPoint Antywirus Suite – szt. 60 na 1 rok, zakup dodatkowych licencji na program antywirusowy ESET EndPoint Antywirus Suite – szt. 60 z ważnością licencji na 1 rok, bądź dostawa rozwiązania równoważnego w ilości 120 szt. z ważnością licencji na 1 rok**,** w rozumieniu pkt II opisu przedmiotu zamówienia,
2. Oferowany program antywirusowy z możliwością ochrony stacji roboczych, urządzeń mobilnych i serwerów będących w posiadaniu Zamawiającego.
3. Zamawiający informuje, że posiadane licencje są ważne do dnia **10.11.2016 r.** i niedopuszczalne jest skrócenie czasu posiadanej licencji na rzecz nowej, dostarczonej przez Wykonawcę.
4. Zamawiający wymaga dołączenia licencji lub klucza aktywacyjnego w formie elektronicznej lub papierowej.
5. Dostawca zobowiązuje się do wydania przedmiotu zamówienia w terminie maksymalnie do 5 dni roboczych od daty podpisania umowy, w przypadku rozwiązania równoważnego, patrz pkt II.

**II. Wymagania dotyczące rozwiązania równoważnego:**

1. Zamawiający dopuszcza możliwość zastosowania przez wykonawców w ofertach rozwiązań kompleksowej ochrony systemów komputerowych opierających się na innym – równoważnym oprogramowaniu, po spełnieniu warunków opisanych poniżej, określających równoważność oprogramowania w stosunku do wskazanego w specyfikacji istotnych warunków zamówienia.
2. Równoważność oprogramowania antywirusowego w stosunku do określonego w specyfikacji istotnych warunków zamówienia – przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań:
   a) oferowane oprogramowanie spełnia specyfikację wymagań z punktu III,
   b) wykonawca wdroży oprogramowanie równoważne w nieprzekraczalnym terminie 3 dni roboczych od zawarcia umowy, czynności wykonywane będą w godzinach pracy zamawiającego,

c) wykonawca przeszkoli personel techniczny (2 osoby) w zakresie używania, zarządzania oraz administrowania programem,

d) wykonawca przygotuje i przekaże zamawiającemu wersję elektroniczną instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze (adekwatnie do liczby licencji),

e) wykonawca dołączy do oferty sporządzoną przez siebie specyfikację funkcjonalną potwierdzającą spełnianie przez oferowane oprogramowanie wymagań określonych w punkcie III.

f) wykonawca w ramach wdrożenia oprogramowania równoważnego przetestuje dostarczane oprogramowanie w kwestii zgodności z oprogramowaniem używanym w SPZOZ w Wieluniu, w celu wykluczenia problemów w funkcjonowaniu dostarczonego oprogramowania i programów użytkowanych w SPZOZ w Wieluniu.

3. Zaproponowany równoważny program antywirusowy musi przejść pozytywne testy w roku 2015 oraz 2016, co najmniej dwa z trzech niezależnych firm testujących rozwiązania antywirusowe:

a) AV-TEST GmbH (www.av-test.org)
b) Virus Bulletin (www.virusbulletin.com)
c) AV-Comparatives (www.av-comparatives.org)

**W przypadku składania oferty równoważnej Zamawiający wymaga złożenia wraz z ofertą co najmniej dwóch wyników testów przeprowadzonych przez ww. firmy testujące rozwiązania antywirusowe.**

## III. Specyfikacja dla oprogramowania równoważnego.

### Wymagania ogólne

1. Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/Windows8/Windows 8.1
2. Wsparcie dla 32 i 64 - bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows w języku polskim
4. Pomoc w programie i dokumentacja do programu dostępna w języku polskim.
5. Skuteczność programu potwierdzona, co najmniej przez dwie niezależne organizacje takie jak:
   a) AV-TEST GmbH (www.av-test.org)
   b) Virus Bulletin (www.virusbulletin.com)
   c) AV-Comparatives (www.av-comparatives.org)

### Ochrona antywirusowa i antyspyware

6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
8. Wbudowana technologia do ochrony przed rootkitami.
9. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
11. 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.
12. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

13. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
14. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
15. Możliwość skanowania dysków sieciowych i dysków przenośnych.
16. Skanowanie plików spakowanych i skompresowanych.
17. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
18. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
19. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
20. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
21. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
22. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
23. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
24. 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.
25. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
26. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail.
27. 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).
28. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
29. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
30. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
31. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
32. 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.
33. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
34. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
35. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

37. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
38. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
39. Aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
40. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
41. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
42. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
43. 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.
44. 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.
45. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
46. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
47. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
48. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
49. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
50. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
51. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
52. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
53. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie samo.
54. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
55. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.

56. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
57. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
58. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
59. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych,pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych
60. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
61. 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.
62. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
63. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
64. Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
65. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
66. Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
    - tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
69. 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.
70. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
71. 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.

72. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
73. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
74. Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
75. Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
76. Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
77. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
78. Aplikacja musi być w pełni zgodna z technologią Network Access Protection (NAP).
79. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
81. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
82. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
83. 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.
84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
85. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna, Obsługa technologii Microsoft NAP.

**Ochrona przed spamem**

86. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird do wersji 5.x wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych.
87. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
88. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird do wersji 5.x – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
89. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
90. 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.
91. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.

92. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
93. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook.
94. 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".
95. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

**Zapora osobista (personal firewall)**

96. Zapora osobista ma pracować jednym z 5 trybów:
    - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące,
    - tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
    - 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.
97. Możliwość tworzenia list sieci zaufanych.
98. Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera.
99. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
100. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
101. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
102. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
103. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
104. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
105. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
106. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
107. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
108. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
109. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
110. 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, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie.

111. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6
112. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
113. Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.

**Kontrola dostępu do stron internetowych**

114. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
115. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
116. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
117. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
118. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
119. 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.
120. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
121. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.

**Konsola administracyjna – zakres funkcjonalny:**

122. Centralna instalacja programów służących do ochrony stacji roboczych Windows.
123. Centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows/ Linux/ MAC OS.
124. Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi typu 2000/XP Professional/Vista/Windows7/Windows 8
125. Do instalacji centralnej i zarządzania centralnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy
126. Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem.
127. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
128. Kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup.
129. Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.

130. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
131. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.
132. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
133. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
134. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
135. Możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.
136. Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
137. Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows Microsoft Windows 8 / 7 / Vista / XP / 2000, Windows Server 2000, 2003, 2008, 2008 R2, 2012, SBS 2003, 2003 R2, 2008, 2011
138. Możliwość rozdzielenia serwera centralnej administracji od konsoli zarządzającej, w taki sposób, że serwer centralnej administracji jest instalowany na jednym serwerze/ stacji a konsola zarządzająca na tym samym serwerze i na stacjach roboczych należących do administratorów.
139. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.
140. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.
141. Serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.
142. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.
143. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.
144. Aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres email.
145. Do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji gdzie jest uruchomiona usługa serwera.
146. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).
147. Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.
148. Serwer centralnej administracji ma umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta,

przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja ma otrzymać odpowiednią konfigurację.

149. Serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę, oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.
150. Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer ma informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych.
151. W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną musi zostać poinformowany o tym fakcie za pomocą okna informacyjnego.
152. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.
153. Aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem szyfrowanej komunikacji (za pomocą protokołu https).
154. Do celu aktualizacji za pośrednictwem protokołu https nie jest wymagane instalowanie dodatkowych zewnętrznych usług jak IIS lub Apache zarówno od strony serwera aktualizacji jak i klienta.
155. Dostęp do kwarantanny klienta ma być z poziomu systemu centralnego zarządzania.
156. Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej administracji.
157. Administrator ma mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej.
158. Podczas przywracania pliku, administrator ma mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.
159. Możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera centralnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.
160. Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi.
161. Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.
162. Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu).
163. W przypadku tworzenia administratora z niestandardowymi uprawnieniami możliwość wyboru modułów, do których ma mieć uprawnienia: zarządzanie grupami, powiadomieniami, politykami,

licencjami oraz usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanna na klientach.

164. Możliwość synchronizowania użytkowników z Active Directory w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania.
165. Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane.
166. Możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej.
167. Panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne.
168. Administrator musi posiadać możliwość tworzenia wielu zakładek, w których będą widoczne wybrane przez administratora elementy monitorujące.
169. Elementy monitorujące muszą umożliwiać podgląd w postaci graficznej co najmniej: bieżącego obciążenia serwera zarządzającego, statusu serwera zarządzającego, obciążenia bazy danych z której korzysta serwer zarządzający, obciążenia komputera, na którym zainstalowana jest usługa serwera zarządzającego, informacji odnośnie komputerów z zainstalowaną aplikacja antywirusową, a które nie są centralnie zarządzane, podsumowania modułu antyspamowego, informacji o klientach znajdujących się w poszczególnych grupach, informacji o klientach z największą ilością zablokowanych stron internetowych, klientach, na których zostały zablokowane urządzenia zewnętrzne, informacje na temat greylistingu, podsumowania wykorzystywanych systemach operacyjnych, informacje odnośnie spamu sms, zagrożeń oraz ataków sieciowych
170. Administrator musi posiadać możliwość maksymalizacji wybranego elementu monitorującego.
171. Możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem.
172. Możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback).
173. Aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności.
174. Wsparcie dla protokołu IPv6
175. Administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej.
176. Centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacji roboczej.
177. Aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu.
178. Aplikacja do administracji centralnej musi umożliwiać utworzenie nośnika, za pomocą którego będzie istniała możliwość przeskanowania dowolnego komputera objętego licencją przed startem systemu.
179. Administrator musi posiadać możliwość określenia ilości jednoczesnych wątków instalacji centralnej oprogramowania klienckiego.

**Użyte przez Zamawiającego wszelkie nazwy handlowe, znaki towarowe, patenty i miejsce pochodzenia są uzasadnione specyfiką przedmiotu zamówienia i mają na celu wskazanie jedynie jakości przedmiotu zamówienia.**

**IV. Nazwa i adres Zamawiającego:**

Nazwa Zamawiającego: **Samodzielny Publiczny Zakład Opieki Zdrowotnej w Wieluniu**
Adres Zamawiającego: **ul. Szpitalna 16**
Kod Miejscowość: **98-300 Wieluń**
Telefon: **43 84 06 800** – **SEKRETARIAT**; **43 84 06 805 – DOiZP**
Faks : **43 84 06 801** – **SEKRETARIAT; 43 84 06 801 – DOiZP**
Adres strony internetowej: **www.szpital.powiat.wielun.pl**

Adres poczty elektronicznej: **sekretariat@szpital-wielun.pl**
**d.surma@szpital-wielun.pl**
Godziny urzędowania: **godziny pracy 7:25-15:00**

**V. Termin wykonania zamówienia:**

1. Termin dostawy przedmiotu zamówienia do dnia 10.11.2016 r..
2. Termin ważności licencji – 12 miesięcy.

**VI. Osoby uprawnione do bezpośredniego kontaktowania się z Wykonawcami:**

stanowisko Administrator Sieci Komputerowej
imię i nazwisko Jarosław Psipsinski
tel. 43 84 06 820
w terminach od poniedziałku do piątku
w godzinach 8:00 – 14.00
e-mail informatycy@szpital-wielun.pl

stanowisko Kierownik Działu Obsługi i Zamówień Publicznych
imię i nazwisko Dariusz Surma
tel. 43 84 06 805
w terminach od poniedziałku do piątku
w godzinach 8:00 – 14.00
e-mail d.surma@szpital-wielun.pl

**VII. Kryterium oceny ofert:**

1. Jedynym kryterium oceny ofert w powyższym postępowaniu jest cena – 100%.
2. Cena oferty musi obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia oraz warunkami stawianymi przez Zamawiającego, uwzględniać wszystkie zobowiązania, podatek od towarów i usług, podatek akcyzowy jeżeli (sprzedaż lub usługa) podlega obciążeniu takimi podatkami, musi być podana w PLN cyfrowo i słownie, zgodnie z Ustawą o cenach z dnia 5 lipca 2001 roku §3 ustęp 1 pkt 1 (Dz. U. 2013 poz. 385 ).

**VIII. Termin, miejsce i forma składania ofert:**

Wyłącznie pisemne oferty należy przesyłać lub składać w zamkniętej kopercie, zabezpieczonej przed przypadkowym otwarciem, z adnotacją na kopercie: **„**Przedłużenie licencji na program antywirusowy ESET– szt. 60 i zakup dodatkowych licencji na program antywirusowy ESET– szt. 60", nr sprawy: SPZOZ-OiZP/2/24/241/ 30 - 19 /2016 **w terminie do dnia 07- 11- 2016 r. do godz. 10.00**
w Sekretariacie SPZOZ w Wieluniu, 98 – 300 Wieluń, ul. Szpitalna 16, pokój nr 216.
Za datę złożenia oferty uważa się datę wpływu do siedziby SPZOZ.
**Oferty złożone po upływie terminu określonego do ich przyjmowania nie będą rozpatrywane.**

**IX. Oferta musi zawierać:**

1. Wypełniony i podpisany Załącznik nr 1 – Formularz ofertowy.
2. Zaparafowany Załącznik nr 2 – Projekt umowy.
3. Aktualny odpis z właściwego rejestru KRS lub Rejestru Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej.

**X. Informacje końcowe:**

1. Zamawiający informuje, że zaproponowane ceny będą porównane z innymi ofertami. Z Wykonawcą, który przedstawi najkorzystniejszą ofertę zostanie podpisana umowa.
2. Zamawiający informuje, że na każdym etapie postępowania może odstąpić od podpisania umowy z Wykonawcą i unieważnić postępowanie.
3. Od decyzji Zamawiającego nie przysługują środki odwoławcze.

p.o. Z-cy Dyrektora
SPZOZ w Wieluniu d/s lecznictwa
dr n. med. Mateusz Grabicki