Świdnik, dnia 30 listopada 2020 r.

Zaproszenie do składania ofert

na przedłużenie licencji oprogramowania antywirusowego

I. Nazwa i adres Zamawiającego:

Sąd Rejonowy Lublin – Wschód w Lublinie
z siedzibą w Świdniku
ul. Kard. S. Wyszyńskiego 18
21-040 Świdnik
tel. 081 46 48 879
/fax 081 46 48 879
e-mail: katarzyna.kwiatkowska@lublin–wschod.sr.gov.pl
NIP: 712-32-35-253
REGON: 060716192
Adres strony internetowej Zamawiającego: www.lublin-wschod.sr.gov.pl
Godziny pracy Sądu:

- od 7:30 do 18:00 (w poniedziałki),
- od 7:30 do 15:30 (od wtorku do piątku).

II. Tryb udzielenia zamówienia:

1. Postępowanie prowadzone jest na podstawie art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (tj. Dz. U. z 2019 r. poz. 1843 ze zm.).
2. Zamawiający zastrzega sobie możliwość:
   a) zmiany postanowień Zaproszenia przed terminem składania ofert,
   b) odwołania niniejszego postępowania bez podania przyczyny – tzw. „unieważnienie postępowania" w każdym czasie do momentu podpisania umowy.
3. Do niniejszego postępowania stosuje się przepisy Kodeksu cywilnego.

III. Nazwa przedmiotu zamówienia:

Przedmiotem zamówienia jest usługa rocznego przedłużenia licencji oprogramowania antywirusowego ESET Suite Endpoint Antivirus NOD32 dla 600 stanowisk.

Zamawiający dopuszcza możliwość zaoferowania dostawy oprogramowania antywirusowego równoważnego (wariant). Poprzez równoważne rozumie się oprogramowanie o funkcjonalności, użyteczności i szybkości działania nie gorszej niż ESET Suite Endpoint Antivirus NOD32 dla 600 stanowisk.

Wykonawca jest zobowiązany do potwierdzenia, że oferowany program antywirusowy jest równoważny poprzez dołączenie do oferty opisu i porównania obu programów. W przypadku zaoferowania oprogramowania równoważnego, **prace związane z dezinstalacją oprogramowania użytkowanego przez Zamawiającego, instalację i wdrożenie dostarczonego oprogramowania na jednostkach komputerowych będą wykonywane przez Wykonawcę w ramach zaoferowanej ceny.**

Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1.

IV. Nomenklatura wg Wspólnego Słownika Zamówień (CPV):

48.76.10.00 – 0 Pakiety oprogramowania antywirusowego

V. Wymagania związane z wykonaniem usługi:

1) Zamawiający wymaga przedłużenia ważności posiadanego klucza licencyjnego na minimum 12 miesięcy (w wariancie przedłużenia). Rozpoczęcie świadczenia usługi nastąpi nie wcześniej niż od dnia 01.01.2021 r. z zastrzeżeniem, że w przypadku dostarczenia licencji na oprogramowanie równoważne prace związane z dezinstalacją oprogramowania użytkowanego przez Zamawiającego, instalację i wdrożenie dostarczonego oprogramowania na jednostkach komputerowych będą wykonywane przez Wykonawcę w ramach zaoferowanej ceny, w sposób umożliwiający świadczenie usługi antywirusowej na warunkach wskazanych w Załączniku Nr 1'
2) w cenie podanej poniżej muszą zostać ujęte wszystkie koszy mające wpływ na realizację przedmiotowego zamówienia m.in. usługi albo koszty dostawy przedłużenia/oprogramowania, licencji, czynności dezintegracji oprogramowania użytkowanego przez Zamawiającego, instalacji, wdrożenia oprogramowania w przypadku, o którym mowa w pkt III.

VI. Ofertę należy:

złożyć w formie pisemnej w terminie do 08 grudnia 2020 r. do godziny 12:00 (osobiście - pok.118 (pierwsze piętro); faksem - 81 46 48 879 lub e-mailem: katarzyna.kwiatkowska@lublin-wschod.sr.gov.pl według wzoru Oferty stanowiącego załącznik nr 2 do Zaproszenia. Zamawiający ma prawo wezwania Wykonawcy do wyjaśnienia treści oferty.

Osoba do kontaktów w sprawie zamówienia: Katarzyna Kwiatkowska.

VII. Kryterium oceny ofert

1. Jedynym kryterium wyboru oferty jest cena. Zamawiający wybierze ofertę najtańszą spośród ofert nie odrzuconych.
2. Cena stanowi 100 % kryterium wyboru. Maksymalną liczbę punktów (100) otrzyma Wykonawca, który zaoferuje najniższą cenę przy jednoczesnym spełnieniu wszystkich innych wymagań określonych w niniejszym zaproszeniu.
3. Oferty budzące wątpliwości mogą być przedmiotem zapytania Zamawiającego o wyjaśnienie ich treści. Zamawiający ma prawo wezwania Wykonawcy do wyjaśnienia treści oferty, a w przypadku braku złożenia wyjaśnień do odrzucenia oferty.
4. W toku oceny ofert Zamawiający może poprawiać w ofercie oczywiste omyłki pisarskie i rachunkowe (z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek) oraz inne omyłki polegające na niezgodności oferty z zaproszeniem, niepowodujące istotnych zmian w treści oferty - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona, z zastrzeżeniem, że ww. czynności Zamawiający wykona przed ustaleniem rankingu ofert.
5. Zamawiający ustali ranking ofert i udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymogom określonym w niniejszym Zaproszeniu oraz w Załącznikach i która została oceniona zgodnie z postanowieniem ppkt 1 jako najkorzystniejsza. W przypadku uchylenia się przez tego Wykonawcę od zawarcia umowy – zostanie wybrana oferta Wykonawcy następnemu w kolejności oferującemu najniższą cenę.

6. W przypadku, gdy dwie lub więcej ofert uzyskała taka sama liczbę punktów, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.
7. Oferty nie spełniające wymogów określonych w postępowaniu będą odrzucane.

VIII. OPIS SPOSOBU OBLICZENIA CENY

1. Pod pojęciem ceny rozumieć należy cenę brutto za całość przedmiotu zamówienia, o którym mowa w pkt. V.
2. W cenie winny być uwzględnione wszystkie inne koszty, jakie powstaną w związku z wykonywaniem dostawy/usługi.

IX. Postanowienia końcowe.

1. W sprawach nieuregulowanych w niniejszym Zaproszeniu mają zastosowanie przepisy Kodeksu cywilnego.
2. Zamawiający zastrzega sobie możliwość odwołania niniejszego postępowania w każdym czasie bez podania przyczyny lub zmiany postanowień Zaproszenia przed terminem składania ofert.
3. Sądem właściwym dla rozpoznawania wszelkich sporów wynikających z niniejszego postępowania jest Sąd Rejonowy Lublin - Zachód z siedzibą w Lublinie albo Sąd Okręgowy w Lublinie.

X. Klauzula informacyjna z art. 13 RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „*RODO*", informuję, że:

1) Administratorem Pani/Pana danych osobowych jest Sąd Rejonowy Lublin-Wschód w Lublinie z siedzibą w Świdniku, ul. Stefana Kardynała Wyszyńskiego 18, 21-040 Świdnik, reprezentowany przez Prezesa lub Dyrektora Sądu w zakresie realizowanych zadań.

2) Może się z Pani/Pan z nami kontaktować poprzez numer telefonu 81 464 87 22.

3) Może się Pani/Pan skontaktować z naszym inspektorem danych osobowych Kamilem Kamińskim w następujący sposób:

a) pod adresem poczty elektronicznej: iod@lublin-wschod.sr.gov.pl

b) pisemnie na adres siedziby Administratora.

4) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c *RODO* w celu związanym z postępowaniem o udzielenie zamówienia publicznego na **„Na przedłużenie licencji oprogramowania antywirusowego" Nr sprawy *LWOG-2402-94/20***, prowadzonym w trybie zaproszenia do złożenia oferty.

5) Dostęp do Pani/Pana danych osobowych mają wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz podmioty współpracujące w zakresie obsługi administracyjnej i informatycznej Sądu Rejonowego Lublin - Wschód w Lublinie z siedzibą w Świdniku.

6) Zebrane dane będą przetwarzane zgodnie z przepisami prawa przez okres niezbędny do realizacji celu dla którego zostały pozyskane i przechowywane w sposób wskazany w instrukcji archiwalnej.

7) Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach *ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 ze zm.), dalej „ustawa Pzp",* związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z *ustawy Pzp*.

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

9) posiada Pani/Pan:

a) na podstawie art. 15 *RODO* prawo dostępu do danych osobowych Pani/Pana dotyczących,

b) na podstawie art. 16 *RODO* prawo do sprostowania Pani/Pana danych osobowych,

c) na podstawie art. 18 *RODO* prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 *RODO*,

d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy *RODO*.

10) nie przysługuje Pani/Panu:

a) w związku z art. 17 ust. 3 lit. b, d lub e *RODO* prawo do usunięcia danych osobowych,

b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 *RODO*,

c) na podstawie art. 21 *RODO* prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c *RODO*.

XI. Wykaz załączników:

a) nr 1 – Szczegółowy opis przedmiotu zamówienia;

b) nr 2 – Formularz Ofertowo - Cenowy;

c) nr 3 – wzór Umowy.

Załącznik nr 1 do Zaproszenia

Szczegółowy Opis przedmiotu zamówienia

1. Pełne wsparcie dla systemu Windows 7/Windows 8.1/Windows 10
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.

Ochrona antywirusowa i antyspyware

5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
7. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
8. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
10. 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.
11. 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).
12. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
13. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
14. Możliwość skanowania dysków sieciowych i dysków przenośnych.
15. Skanowanie plików spakowanych i skompresowanych.
16. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
17. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
18. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
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 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 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 opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.

31. 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.

32. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.

33. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

34. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

35. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

36. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.

37. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.

38. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

39. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.

40. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.

41. 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.

42. 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.

43. 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.

44. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.

45. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

46. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

47. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

48. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.

49. 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.

50. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.

51. 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.

52. 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.

53. 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.

54. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.

55. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.

56. 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.

57. 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.

58. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.

59. 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.

60. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

61. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

62. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika

63. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

64. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

- tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
- Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

65. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

66. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

67. Oprogramowanie musi posiadać zaawansowany skaner pamięci.

68. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.

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. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.

75. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.

76. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http

77. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).

78. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

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 program włączał 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, 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. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.

86. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.

87. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.

88. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
89. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
90. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.
91. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny
92. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
93. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.
94. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.
95. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
96. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
97. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami i exploitami.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
9. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
10. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.

13. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. 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.
15. Aplikacja powinna wspierać mechanizm klastrowania.
16. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
17. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
18. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
19. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
20. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
21. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
22. 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.
23. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
24. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
25. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
26. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
27. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
28. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
29. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
30. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
31. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
32. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
33. 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.

34. 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.

35. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.

36. Aktualizacje modułów analizy heurystycznej.

37. 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.

38. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

39. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.

40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

42. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.

43. 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.

44. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.

45. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.

46. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.

47. 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.

48. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.

49. 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.
50. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
52. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
53. 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.
54. 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.
55. 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.
56. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
57. 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).
58. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
59. 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).
60. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
61. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
62. Aplikacja musi wspierać skanowanie magazynu Hyper-V
63. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
64. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie procesu ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki.
65. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
66. Praca programu musi być niezauważalna dla użytkownika.

67. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
68. 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 2008R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 oraz systemach Linux.
2. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
3. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
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 administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
7. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
8. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
9. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
10. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
11. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
12. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
13. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
14. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
15. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
16. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
17. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
18. 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.

19. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
20. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
21. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
22. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
24. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
25. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
26. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
27. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej
28. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
29. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
30. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
31. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
32. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
33. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
34. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
35. 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.
36. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.

37. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
38. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
39. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
40. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
41. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
42. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
43. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
44. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
45. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
46. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
47. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
48. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
49. 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.
50. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
51. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
52. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
53. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
54. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
55. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.

56. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.

57. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.

58. 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.

59. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.

60. 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.

61. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.

62. 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.

63. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.

64. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta

65. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.

66. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.

67. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.

68. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.

69. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.

70. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.

71. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.

72. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
73. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
74. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
75. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
76. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
77. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
78. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
79. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
80. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
81. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
82. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
83. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
84. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
85. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
86. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
87. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
88. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.

89. 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.

90. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli.

91. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie.

92. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli.

93. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.

94. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.

Załącznik nr 2 do Zaproszenia

OFERTA

1. Pełna nazwa Wykonawcy:
   ……
   ……
2. NIP: ……..
   REGON: ……
3. Adres siedziby Wykonawcy:
   ……
   ……
4. Adres korespondencyjny:
   ……
   ……
5. Telefon:
   ……
6. Fax.:
   ……
7. E-mail:
   ……
8. **Oferuję wykonanie przedmiotu zamówienia za:**

	/Usługa przedłużenia licencji/Oprogramowanie	**Producent oprogramowania**	**Nazwa programu**	**Ilość licencji**	**Cena brutto 1 licencji**	**Cena brutto**
a	***b***	***c***	***d***	***e***	***f***	***g = e x f***
1.	**Przedłużenie licencji Eset Suite Endpoint Antivirus NOD32 /równoważne w postaci dostawy ……..…***			**600**		

****nieodpowiednie skreślić***

<u>Ponadto deklaruję:</u>

a) **termin realizacji Umowy w zakresie ochrony antywirusowej - od 01 stycznia 2021 r. do dnia 31 grudnia 2021 r.;**
b) **warunki płatności: zgodnie ze wzorem Umowy;**
c) **gwarancja i rękojmia – od dnia 01 stycznia 2021 r. do dnia 31 grudnia 2021 r.**

9. **Oświadczam/y, że:** powyższa cena zawiera wszystkie koszty wykonania zamówienia i realizacji przyszłego świadczenia umownego.
10. Zapoznałem/am się/zapoznaliśmy się z postanowieniami Zaproszenia do składania ofert i nie wnoszę/wnosimy żadnych zastrzeżeń oraz uzyskałem/am /uzyskaliśmy konieczne informacje do przygotowania oferty.
11. Uważam/y się za związanych niniejszą ofertą przez okres 30 dni licząc od dnia wyznaczonego jako termin składania ofert.
12. Zawarty wzór umowy (załącznik nr 3) został przeze mnie/przez nas zaakceptowany i zobowiązuję/my się w przypadku wyboru naszej oferty do zawarcia umowy zgodnej z tym wzorem umowy, w miejscu i terminie wyznaczonym przez Zamawiającego.
13. **Oświadczam, iż w przypadku oprogramowania równoważnego, że oprogramowanie posiada funkcjonalności, użyteczność i szybkości działania nie gorszą niż oprogramowania wskazane pierwotnie przez Zamawiającego względem których należało odnieść równoważność.***

nieodpowiednie skreślić

……, dnia ……..

……

podpis osoby uprawnionej

Załącznik nr 3 do Zaproszenia

WZÓR

UMOWA NR ……

z dnia ……..

Niniejsza umowa, zwana dalej **„Umową”** została zawarta po przeprowadzeniu postępowania o zamówienie publiczne na podstawie art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 ze zm.) pomiędzy:

Skarbem Państwa – Sądem Rejonowym Lublin – Wschód w Lublinie z siedzibą w Świdniku

21-040 Świdnik, ul. Kard. S. Wyszyńskiego 18

NIP: 712-32-35-253, REGON: 060716192

reprezentowanym przez:

.....

zwanym dalej w treści Umowy **„Zamawiającym”**

a

.....

z siedzibą w ....., przy ul. .....,

wpisaną/ym do rejestru KRS .....

NIP: ……REGON……..

reprezentowaną/ym przez:

1) .....

2) .....

zwaną/ym dalej w treści Umowy **„Wykonawcą”**

PRZEDMIOT ZAMÓWIENIA

§ 1.

1. **Zamawiający** zleca, a **Wykonawca** przyjmuje do realizacji zadanie pt. „Przedłużenie licencji/dostawę oprogramowania antywirusowego”.

2. Wykonawca w ramach przedmiotu zamówienia:

1) przedłuży licencje na oprogramowanie antywirusowe ESET Endpoint Antivirus NOD32 dla 600 stanowisk*;

2) dostarczy oprogramowanie antywirusowe z roczną licencją równoważną do oprogramowania antywirusowego ESET Endpoint Antivirus NOD32 dla 600 stanowisk*;

oraz wykona czynności dezintegracji oprogramowania użytkowanego przez Zamawiającego oraz instalacji i wdrożenia dostarczonego oprogramowania*.

3. Wykonawca przedłuży licencje/dostarczy oprogramowanie* **w terminie do dnia 01.01.2021 r.** W przypadku dostarczenia licencji na oprogramowanie równoważne prace związane z dezinstalacją oprogramowania użytkowanego przez Zamawiającego, instalację i wdrożenie dostarczonego oprogramowania na jednostkach komputerowych będą wykonywane przez Wykonawcę w ramach zaoferowanej ceny, w sposób umożliwiający świadczenie usługi antywirusowej na warunkach wskazanych w Załączniku Nr 1 od daty wskazanej w zdaniu 1*, a w przypadku oferty wariantowej zrealizuje usługi w postaci: dezinstalacji oprogramowania.

**** Nieodpowiednie skreślić w zależności od oferty Wykonawcy***

ZASADY REALIZACJI

§ 2.

1. Wykonawca zapewnia na podstawie licencji działanie oprogramowania antywirusowego przez okres od dnia 01.01.2021 r. do dnia 31.12.2021 r.

2. Wykonawca zapewnia, że przedmiot zamówienia jest nowy, wolny od wad fizycznych i prawnych oraz nie jest przedmiotem praw osób trzecich.

WYNAGRODZENIE

§ 3.

1. Strony ustaliły wynagrodzenie ryczałtowe w wysokości netto **……..** (słownie: ……).

Cena określona w ust. 1 jest ceną stałą i nie może być podwyższona. Obejmuje wszelkie koszty związane z realizacją zamówienia, w tym koszty wynikające z § 4 Umowy, a w przypadku dostarczenia licencji na oprogramowanie równoważne wynagrodzenie za prace związane z dezinstalacją oprogramowania użytkowanego przez Zamawiającego, instalację i wdrożenie dostarczonego oprogramowania*.

**** Nieodpowiednie skreślić w zależności od oferty Wykonawcy***

2. Do ceny, o której mowa w ust. 1 zostanie dodany podatek VAT zgodnie z obowiązującymi przepisami prawa.

3. Wynagrodzenie płatne będzie po wykonaniu przedmiotu zamówienia, o którym mowa w § 1 ust. 2 w zw. z ust. 3 na podstawie prawidłowo wystawionej faktury VAT w terminie do 21 dni od dnia jej doręczenia Zamawiającemu, z zastrzeżeniem, że Wykonawca ma prawo wystawienia faktury po podpisaniu protokołu odbioru kluczy licencyjnych bez zastrzeżeń.

4. Za datę dokonania płatności Strony będą uważały datę przekazania przez Zamawiającego zlecenia przelewu do banku obsługującego.

5. Wszelkie płatności dokonywane będą w złotych polskich.

6. Zamawiający akceptuje wystawianie i dostarczanie w formie elektronicznej, w formacie PDF: faktur, faktur korygujących oraz duplikatów faktur, zgodnie z art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz.U. z 2020 r. poz. 106 ze zm.) w zw. z ustawą z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz.U. z 2018 r. poz. 2191).

7. Zamawiający będzie stosował mechanizm podzielonej płatności. Podzieloną płatność, tzw. split payment stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata odszkodowania), a także za świadczenia zwolnione z VAT, opodatkowane stawką 0% lub objęte odwrotnym obciążeniem. Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności.

OBOWIĄZKI WYKONAWCY

§ 4.

1. Wykonawca zobowiązuje się wykonać usługę przedłużenia licencji on-line/dostarczyć zamówione

oprogramowanie do siedziby Zamawiającego w terminach wskazanych w Umowie oraz zgodnie ze Szczegółowy Opisem Przedmiotu Zamówienia do Zaproszenia*.

**** Nieodpowiednie skreślić w zależności od oferty Wykonawcy***

2. Wykonawca zobowiązany jest dostarczyć wszystkie dokumenty poświadczające parametry oraz licencje dotyczące przedmiotu zamówienia wymagane przez Zamawiającego.

3. Za datę wykonania przedmiotu zamówienia uważa się datę podpisania protokołu odbioru przez upoważnionego przedstawiciela Zamawiającego.

4. W przypadku stwierdzenia nienależytego wykonania przedmiotu umowy stwierdzonego w trakcie odbioru Zamawiający zgłosi zastrzeżenia Wykonawcy. Wykonawca jest obwiązany usunąć wady stwierdzone w trakcie odbioru w terminie 2 dni roboczych.

5. Wykonawca gwarantuje telefoniczne wsparcie w języku polskim dostępne w dni robocze od godziny 10:00 do 15:30 zapewnione przez producenta oprogramowania lub Wykonawcę.

6. W przypadku zgłoszenia problemu z aplikacją Wykonawca zapewni rozwiązanie problemu nie później niż 24 h od zgłoszenia.

ODPOWIEDZIALNOŚĆ WYKONAWCY

§ 5.

1. W przypadku niewykonania przez Wykonawcę lub nienależytego wykonania niniejszej Umowy Zamawiającemu przysługują kary umowne:

a) w przypadku opóźnienia w wykonaniu przedmiotu Umowy w terminie określonym w § 1 ust. 3 Umowy – 200.00 zł (słownie: dwieście zł 00/100) za każdy dzień opóźnienia;

b) w przypadku opóźnienia w usunięciu wad stwierdzonych przy odbiorze lub w okresie rękojmi i gwarancji jakości za wady względem terminów odpowiednio, o których mowa w § 4 ust. 4 lub wyznaczonych przez Zamawiającego - 100.00 zł (słownie: sto zł 00/100) za każdy dzień opóźnienia;

c) w przypadku opóźnienia w rozwiązaniu problemu względem terminu, o którym mowa w § 4 ust. 6 - 300.00 zł (słownie: trzysta zł 00/100) za każdy dzień opóźnienia liczonego od dnia wyznaczonego przez Zamawiającego;

d) w przypadku odstąpienia przez Wykonawcę od Umowy z przyczyn nie leżących po stronie Zamawiającego – 2 000.00 zł (słownie: dwa tysiące zł 00/100);

e) w przypadku odstąpienia przez Zamawiającego od Umowy z przyczyn leżących po stronie Wykonawcy - 2 000.00 zł (słownie: dwa tysiące zł 00/100).

2. Zamawiający ma prawo odstąpienia od Umowy ze skutkiem natychmiastowym do czasu upływu okresu obowiązywania Umowy, bez dodatkowego wezwania, gdy Wykonawca nie wypełnia postanowień niniejszej Umowy, w szczególności gdy narusza postanowienia § 2 ust. 3 popadając w opóźnienie powyżej 3 dni roboczych lub § 4 ust. 4 popadając w opóźnienie powyżej 3 dni roboczych.

3. Zamawiający ma prawo do naliczania kar umownych, o których mowa w ust. 1 lit. a) do c) niezależnie od skorzystania z prawa odstąpienia od Umowy z powodu tych samych okoliczności, które były podstawą naliczenia kar, oraz niezależnie od kary umownej przysługującej Zamawiającemu zgodnie z ust. 1 lit. d) lub e). Łączna wysokość kar umownych nie może przekroczyć 50 % wartości brutto wynagrodzenia Wykonawcy.

4. Zamawiający ma prawo potrącenia należności z tytułu kar, o których mowa w ust. 1 lit. a) – e),

z należnego Wykonawcy wynagrodzenia.

5. Zamawiający ma prawo dochodzenia odszkodowania uzupełniającego przenoszącego wysokość kar umownych, na zasadach ogólnych.

ODPOWIEDZIALNOŚĆ ZA WADY

§ 6.

1. Wykonawca udziela Zamawiającemu gwarancji na przedmiot umowy, o którym mowa w § 1 ust. 2 na okres od dnia 01 grudnia 2021 r. do dnia 31 grudnia 2021 r.
2. Okres rękojmi jest równy okresowi gwarancji.
3. Zamawiający może według własnego wyboru skorzystać z uprawnień wynikających z gwarancji jakości lub rękojmi.

OKRES OBOWIĄZYWANIA

§ 7.

Umowę zawiera się na czas określony dnia 31 grudnia 2021 r.

POSTANOWIENIA KOŃCOWE

§ 8.

1. Osobą odpowiedzialną za bieżący kontakt z Wykonawcą po stronie Zamawiającego w tym podpisanie protokołu odbioru, o którym mowa w § 4 ust. 3 jest:
   a) ……..
2. Osobą odpowiedzialną za bieżący kontakt z Zamawiającym po stronie Wykonawcy w tym podpisanie protokołu odbioru, o którym mowa w § 4 ust. 3 jest:
   a) ……
3. Zmiana osób wskazanych w ust. 1 i 2 nie wymaga aneksu do umowy i nastąpi poprzez pisemne poinformowanie stron na piśmie.

KLAZULA POUFNOŚCI, ZAKAZ CESJI

§ 9.

1. Wykonawca zobowiązany jest do zachowania w tajemnicy wszelkich informacji, w posiadanie których wszedł wykonując przedmiot Umowy.
2. Wykonawcy nie wolno dokonać cesji wierzytelności wynikających z niniejszej Umowy bez zgody Zamawiającego wyrażonej pod rygorem nieważności na piśmie.

POZOSTAŁE POSTANOWIENIA

§ 10.

1. Strony zobowiązują się do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa.
2. Dane osobowe, o których mowa w Umowie udostępniane są przez Strony w celu realizacji Umowy, na podstawie art. 6 ust. 1 lit. b) i c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

3. Strony zobowiązuje się do udzielenia drugiej Stronie oraz innym podmiotom uprawnionym na podstawie przepisów prawa, na każde ich żądanie, informacji na temat przetwarzania danych osobowych udostępnionych przez druga Stronę w związku z realizacją Umowy.
4. Strony zobowiązane są do zastosowania się do zabezpieczenia powierzonych do przetwarzania danych osobowych.
5. Wykonawca oświadcza, że uzyskał od Zamawiającego informacje zgodnie z art. 13 RODO, które to Zamawiający zamieścił w Zaproszeniu.

§ 11.

1. Wszelkie zmiany postanowień Umowy wymagają dla swej ważności formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają przepisy Kodeksu Cywilnego, a w sprawach formalnoprawnych przepisy kodeksu postępowania cywilnego.
3. Obie strony oświadczają, że spory wynikające z Umowy będzie rozstrzygał w zależności od wartości przedmiotu sporu Sąd Rejonowy Lublin-Zachód w Lublinie albo Sąd Okręgowy.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, jeden egzemplarz dla Wykonawcy, jeden egzemplarz dla Zamawiającego.
5. Integralną częścią niniejszej umowy jest Oferta Wykonawcy z dnia …….

ZAMAWIAJĄCY	WYKONAWCA

Załącznik nr 2 do Umowy

Wzór protokołu odbiorczego

Sporządzony w dniu _____ r. w _____
pomiędzy:
Zamawiającym:
Skarb Państwa - Sądem Rejonowym Lublin – Wschód w Lublinie z siedzibą w Świdniku, reprezentowany przez _____
a
Wykonawcą:
_____
reprezentowanym/ą przez_____

Stwierdzamy, że zamówiony przedmiot Umowy został wykonany zgodnie/niezgodnie* z Umową Nr LWOG-2403-_____ /2020 r. z dnia _____ .

W przypadku niezgodności –zastrzeżenia Zamawiającego*:
……
……
……
……
……
……

*odpowiednie skreślić

ZAMAWIAJĄCY	WYKONAWCA