Dostawa oprogramowania antywirusowego oraz zapewnienie ciągłości aktualizacji przez okres 3 lat
Szczegółowy Opis Przedmiotu Zamówienia

Słownik

1. stanowisko robocze – komputery stacjonarne i notebooki użytkowane przez Zamawiającego
2. system antywirusowy – wszystkie komponenty programowe dostarczone przez Wykonawcę służące do ochrony antywirusowej
3. centralne zarządzanie systemem antywirusowym – zarządzanie wszystkimi komponentami oprogramowania antywirusowego z „jednego miejsca" – za pomocą konsoli ekranowej
4. serwer centralnego zarządzania – komputer, na którym zainstalowana jest część serwerowa oprogramowania służąca do realizacji centralnego zarządzania systemem antywirusowym
5. ciągłości aktualizacji sygnatur wirusowych – możliwość pobrania aktualnych sygnatur wirusowych nie rzadziej niż co 24h
6. niezależne laboratorium – laboratorium z siedzibą na terenie Unii Europejskiej, nie związane organizacyjnie z producentem oprogramowania, publikujące wyniki badań na ogólnie dostępnych stronach internetowych minimum od roku 2015; wyniki badań muszą być publikowane w języku polskim lub angielskim; publikowane raporty muszą dotyczyć minimum 5 programów antywirusowych
7. klient – stacja robocza, smartfon lub serwer z zainstalowanym oprogramowaniem antywirusowym wchodzącym w skład systemu antywirusowego

Specyfikacja

1. **Wymagania w zakresie obsługiwanych platform systemowych**
   - 1.1. Oprogramowanie przeznaczone do ochrony stanowisk roboczych musi poprawnie funkcjonować na platformach:
     - 1.1.1. Microsoft Windows XP Professional x86 Edition SP3
     - 1.1.2. Microsoft Windows Vista® x86 Edition SP2
     - 1.1.3. Microsoft Windows 7 Professional
     - 1.1.4. Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
     - 1.1.5. Microsoft Windows 8 Pro x86
     - 1.1.6. Microsoft Windows 8 Pro x64
     - 1.1.7. Microsoft Windows 8.1 Pro x86
     - 1.1.8. Microsoft Windows 8.1 Pro x64
     - 1.1.9. Microsoft Windows 10 Pro x86
     - 1.1.10. Microsoft Windows 10 Pro x64
   - 1.2. Oprogramowanie do ochrony smartfonów musi poprawnie funkcjonować na platformie Android
   - 1.3. Oprogramowanie przeznaczone do ochrony serwerów musi poprawnie funkcjonować na platformach:
     - 1.3.1. Microsoft Windows Server 2003 (wszystkie edycje)
     - 1.3.2. Microsoft Windows Server 2003 x64 (wszystkie edycje)
     - 1.3.3. Microsoft Windows Server 2008 (wszystkie edycje)
     - 1.3.4. Microsoft Windows Server 2008 x64 (wszystkie edycje)
     - 1.3.5. Microsoft Windows Server 2008 R2 (wszystkie edycje)
     - 1.3.6. Microsoft Windows Server 2012 (wszystkie edycje)
     - 1.3.7. Microsoft Windows Server 2012 R2 (wszystkie edycje)
     - 1.3.8. Linux kernel 2.6 lub nowszy
   - 1.4. Oprogramowanie służące do centralnego zarządzania systemem antywirusowym - serwer centralnego zarządzania musi poprawnie funkcjonować na platformach MS Windows Server (przynajmniej tych, które zostały wymienione w pkt. 1.3.3 do 1.3.7)
   - 1.5. Oprogramowanie służące do centralnego zarządzania systemem antywirusowym - konsola centralnego zarządzania musi poprawnie funkcjonować na platformie MS Windows

przeznaczonych do pracy na stanowiskach roboczych i serwerach (przynajmniej jednej z wymienionych w pkt. od 1.1.3 do 1.1.10 oraz w pkt. od 1.3.3 do 1.3.7).

2. **Wymagania w zakresie wersji językowej dotyczące wszystkich komponentów systemu antywirusowego, dokumentacji i wsparcia technicznego:**
   2.1. Wersja programu dla stacji roboczych i serwerów w języku polskim
   2.2. Pomoc w programie w języku polskim
   2.3. Dokumentacja w języku polskim
   2.4. Wsparcie techniczne do programu świadczone w języku polskim przez dystrybutora autoryzowanego przez producenta programu.
3. **Wymagania w zakresie ilości licencji i funkcjonalności:**
   3.1. Dostawa 1100 licencji ESET Secure Enterprise AV Level dla komputerów lub oprogramowania równoważnego spełniającego następujące wymagania:
   3.1.1. W ramach dostarczonej licencji muszą zostać zabezpieczone minimum 84 urządzenia mobilne z systemem Android, które posiada Zamawiający
   3.1.2. Zapewnienie ciągłości aktualizacji sygnatur wirusowych przez pełny okres ważności licencji
   3.1.3. Zapewnienie ochrony przed wirusami, trojanami, „robakami komputerowymi", itp.
   3.1.4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu Adware, Spyware, Dialer, phishing, narzędzi hakerskich, backdoor, itp.
   3.1.5. Wbudowana technologia do ochrony przed rootkitami
   3.1.6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu
   3.1.7. Skanowanie dysków sieciowych i dysków przenośnych
   3.1.8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym
   3.1.9. Definiowanie listy rozszerzeń plików, które mają być skanowane, z uwzględnieniem plików bez rozszerzeń
   3.1.10. Dodawania do listy wyłączeń ze skanowania wybranych plików, katalogów lub rozszerzeń
   3.1.11. Wbudowany konektor dla programów MS Outlook wersje: 2007, 2010, 2013, 2016
   3.1.12. Skanowanie całej poczty przychodzącej i wychodzącej odbieranej przy pomocy programu MS Outlook
   3.1.13. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej – niezależnie od klienta pocztowego
   3.1.14. Możliwość opcjonalnego dołączenia do każdej odbieranej wiadomości lub tylko do zainfekowanych wiadomości e-mail informacji o jej przeskanowaniu
   3.1.15. Skanowanie ruchu HTTP na stacjach roboczych
   3.1.16. Blokowanie możliwości otwierania zdefiniowanych przez administratora stron internetowych. Program musi umożliwić blokadę całej nazwy witryny i na wybrane słowo występujące w nazwie witryny
   3.1.17. Automatyczna integracja skanera POP3 i HTTP z dowolnym klientem pocztowym i dowolną przeglądarką internetową, niewymagająca zmian w konfiguracji
   3.1.18. Możliwość definiowania różnych portów POP3 i HTTP, na których ma odbywać się skanowanie
   3.1.19. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików
   3.1.20. Skanowanie baz MS Outlook-a wersje: 2007, 2010, 2013, 2016
   3.1.21. Skanowanie plików spakowanych i skompresowanych
   3.1.22. Możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności)
   3.1.23. Możliwość wyłączenia skanowania przy pomocy baz sygnatur wirusów, w takim przypadku oprogramowanie ma skanować jedynie algorytmami heurystycznymi

3.1.24. Możliwość wysyłania wraz z próbką swojego komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia
3.1.25. Wysyłanie zagrożeń do laboratorium ma odbywać się przy pomocy serwera centralnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych
3.1.26. Przesuwanie zainfekowanych plików i załączników poczty w bezpieczny obszar stacji (do katalogu kwarantanny) w celu dalszej kontroli
3.1.27. Możliwość ręcznego wysłania próbki z kwarantanny do laboratorium producenta dodając opis i adres zwrotny (e-mail)
3.1.28. Program powinien posiadać certyfikaty niezależnych laboratoriów
3.1.29. W przypadku wykrycia wirusa, oprogramowanie musi informować - ostrzegać użytkownika i administratora
3.1.30. Prowadzenie dziennika zdarzeń rejestrującego informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania
3.1.31. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu
3.1.32. Możliwość zabezpieczenia hasłem wyłączenia programu antywirusowego i poszczególnych funkcji programu
3.1.33. Automatyczna aktualizacja baz sygnatur wirusów i innych zagrożeń
3.1.34. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, bądź CD ROM-u, a także przy pomocy HTTP z dowolnej stacji roboczej lub serwera
3.1.35. 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)
3.1.36. Możliwość przypisania minimum 2 profili z różnymi ustawieniami do jednego zadania aktualizacji np. podst. profil aktualizuje z sieci lokalnej po http a zapasowy z Internetu. Drugi jest używany, gdy pierwszy nie działa
3.1.37. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji
3.1.38. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line)
3.1.39. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło
3.1.40. 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
3.1.41. 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, powinna także istnieć opcja dezaktywacji tego mechanizmu
3.1.42. Użytkownik powinien 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
3.1.43. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusowych z Internetu lub z bazy zapisanej na dysku
3.1.44. System antywirusowy powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: portów USB
3.1.45. Funkcja blokowania portów USB powinna umożliwiać administratorowi zdefiniowanie listy portów USB w komputerze, które nie będą blokowane (wyjątki)
3.1.46. System antywirusowy powinien posiadać 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

3.2. Dostawa licencji dla 1100 skrzynek pocztowych ESET Mail Security for MS Exchange lub oprogramowania równoważnego o następujących wymaganiach:

3.2.1. Wsparcie dla MS Exchange 2010 oraz 2013
3.2.2. Wsparcie dla ról Mailbox, Edge, Hub
3.2.3. Skanowanie poczty przychodzącej i wychodzącej na serwerze MS Exchange
3.2.4. Program powinien zapewnić skanowanie bezpośrednio w storach MS Exchange przy pomocy VSAPI 2.6 lub nowszym
3.2.5. Program ma zapewnić skanowanie przed zapisaniem wiadomości w storze przy pomocy transport agenta
3.2.6. W przypadku wykrycia wirusa/blokowania wiadomości system musi umożliwić usuniecie wiadomości/ załącznika, wyleczenie, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji
3.2.7. Możliwość tworzenia różnych reguł blokowania wiadomości po zdefiniowanym nadawcy, odbiorcy, temacie, treści, nazwie załącznika i wielkości wiadomości
3.2.8. Możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail
3.2.9. Wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty
3.2.10. Konfiguracja filtra antyspamowego powinna znajdować się w innym pliku konfiguracyjnym niż konfiguracja skanera antywirusowego, można edytować ten plik, aby dokonać dokładnej konfiguracji
3.2.11. Producent programu powinien wyposażyć program w przynajmniej 3 predefiniowane profile systemu antyspamowego
3.2.12. System antyspamowy powinien być wyposażony przynajmniej w filtr Bayesa, sprawdzanie list RBL oraz mechanizm reputacji poczty
3.2.13. Program powinien posiadać mechanizmy greylistingu (szare listy)
3.2.14. System musi umożliwiać ustawienie jednego z 5 poziomów logowania błędów
3.2.15. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu
3.2.16. Wykrywanie niebezpiecznych aplikacji typu Adware, Spyware, Dialer itp.
3.2.17. Wbudowana technologia do ochrony przed rootkitami
3.2.18. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym
3.2.19. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików
3.2.20. Skanowanie plików spakowanych i skompresowanych
3.2.21. Skanowanie ruchu HTTP lokalnego serwera. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie
3.2.22. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie
3.2.23. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS i POP3S
3.2.24. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe
3.2.25. Administrator powinien mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego
3.2.26. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy minimum programu MS Outlook
3.2.27. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego)
3.2.28. Automatyczna integracja skanera POP3 z klientem pocztowym MS Outlook bez konieczności zmian w konfiguracji
3.2.29. Możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie

3.2.30. Możliwość wyłączenia skanowania przy pomocy bazy sygnatur wirusowych (skanowanie samą heurystyką)
3.2.31. Używanie heurystycznych metod do wykrywania infekcji
3.2.32. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy – nie wymaga ingerencji użytkownika
3.2.33. Możliwość wysyłania wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia
3.2.34. W przypadku wykrycia wirusa oprogramowanie musi informować - ostrzegać administratora
3.2.35. Prowadzenie dziennika zdarzeń rejestrującego informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania
3.2.36. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu
3.2.37. Możliwość zabezpieczenia hasłem wyłączenia programu antywirusowego oraz jego odinstalowania
3.2.38. Automatyczna aktualizacja baz sygnatur wirusów i innych zagrożeń
3.2.39. 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)
3.2.40. 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, profil zapasowy w przypadku niepowodzenia aktualizacji z profilu głównego)
3.2.41. Skuteczność programu powinna być potwierdzona nagrodami lub certyfikatami niezależnych laboratoriów

4. Wymagania w zakresie centralnego zarządzania systemem antywirusowym:

4.1. Możliwość centralnego zarządzania oprogramowaniem antywirusowym wchodzącym w skład systemu uruchomionym na stacjach roboczych i serwerach
4.2. Z poziomu serwera zarządzającego musi być możliwość sprawdzenia stanu ochrony, wersji bazy wirusów, wyników skanowania skanera na żądanie i rezydentnych monitorów
4.3. Z poziomu serwera zarządzającego można zobaczyć adres IP, MAC adres, wersje systemu operacyjnego, domenę do której należy stacja
4.4. Zmiana konfiguracji na stacjach i serwerach jest możliwa z konsoli centralnego zarządzania lub lokalne, jeśli użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne
4.5. Centralna konfiguracja i zarządzanie programami antywirusowymi, modułem antyspamowym zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera centralnego zarządzania
4.6. Zdalna instalacja ochrony antywirusowej na stacjach roboczych
4.7. Możliwość tworzenia grup stacji roboczych z oddzielnymi ustawieniami konfiguracyjnymi.
4.8. Możliwość importowania konfiguracji programu antywirusowego wybranej stacji roboczej, a następnie przesłanie jej na inną stację lub grupę stacji roboczych w sieci
4.9. Zdalne skanowanie stacji roboczych z możliwością wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej
4.10. Skanowanie sieci w poszukiwaniu niezabezpieczonych stacji roboczych
4.11. Automatyczne generowanie raportów (w ustalonych odstępach czasu) lub na żądanie do plików HTML lub eksportowanych do pliku CSV
4.12. Zbieranie wszystkich alertów i informacji (baza wirusów, stan monitora, data ostatniej aktualizacji, wersja systemu operacyjnego, adres IP)
4.13. Możliwość tworzenia kilku serwerów zarządzających i replikowania ich między sobą w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta)
4.14. Serwer centralnego zarządzania musi mieć możliwość generowania repozytorium aktualizacji i udostępnianie go przez wbudowany serwer http

4.15. Serwer centralnego zarządzania powinien 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
4.16. Serwer centralnego zarządzania powinien być wyposażony w mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji używanych przez użytkownika
4.17. Dostęp do kwarantanny klienta z poziomu systemu centralnego zarządzania
4.18. Aktualizacja baz sygnatur wirusowych i innych zagrożeń powinna odbywać się przynajmniej raz dziennie
4.19. Wszystkie komponenty muszą współpracować z jedną konsolą zarządzającą
4.20. Wszystkie komponenty muszą pochodzić od jednego producenta
4.21. Licencja powinna dawać możliwość korzystania z serwisu technicznego z zakresu instalacji i użytkowania oprogramowania i dostępu do internetowej aktualizacji baz sygnatur wirusowych bez ponoszenia dodatkowych kosztów
4.22. Licencja musi dawać prawo i możliwość nielimitowanego centralnego zarządzania wszystkimi komponentami zakupionego systemu antywirusowego.

5. Wymagania w zakresie ochrony urządzeń mobilnych z systemem Android:
5.1. Skanowanie nowych aplikacji przed ich uruchomieniem
5.2. Skanowanie plików wykonywalnych, minimum takich jak: EXE, APK
5.3. Skanowanie archiwów minimum takich jak: ZIP, JAR
5.4. Skanowanie wszystkich otwieranych, modyfikowanych, przenoszonych, kopiowanych, uruchamianych oraz zapisywanych plików na urządzeniu przez użytkownika
5.5. Określanie akcji jaka ma zostać wykonana wobec wykrytego obiektu w sytuacji gdy leczenie nie jest możliwe
5.6. Włączenie lub wyłączenie pobierania aktualizacji w roamingu
5.7. Możliwość ręcznego zdefiniowania źródła aktualizacji
5.8. Możliwość określenia akcji w przypadku zaistnienia zdarzenia oraz przesyłanie informacji o ich zaistnieniu do administratora systemu.

6. Wymagania w przypadku zaoferowania rozwiązania równoważnego:
6.1. Wykonawca musi w uzgodnieniu z Zamawiającym zaproponować procedurę i udzielić mu wsparcia tak aby zagwarantować sprawne przeprowadzenia procesu odinstalowania obecnie używanego produktu oraz instalację i uruchomienie dostarczonego oprogramowania na wszystkich wskazanych przez Zamawiającego stacjach roboczych i serwerach, do niego należących. Działanie to musi zapewnić ciągłość zabezpieczenia antywirusowego w/w stacji roboczych i serwerów. Uwaga: Zamawiający posiada licencję na oprogramowanie antywirusowe ważną do dnia 2016.06.25.

7. Wymagania w zakresie terminu ważności licencji:
7.1. Wykonawca musi dostarczyć oprogramowanie w taki sposób aby osiągnęło ono opisaną w SOPZ funkcjonalność nie później niż 2016.06.17
7.2. Ważność licencji na dostarczone oprogramowanie musi rozpocząć się nie później niż dnia 2016.06.26. i trwać nie krócej niż do dnia 2019.06.26.

8. Wymagania w zakresie szkoleń:
8.1. Wykonawca musi przeszkolić minimum 2 osoby - administratorów wskazane przez Zamawiającego
8.2. Szkolenie musi zostać przeprowadzone w wymiarze nie krótszym niż 16 godzin, przy czym jedno szkolenie nie może trwać dłużej niż 8 godzin
8.3. Harmonogram oraz miejsce szkoleń musi zostać uzgodniony z Zamawiającym
8.4. Pełny wymiar czasowy szkolenia musi zostać wykonany nie później niż do września 2016r.

9. Wymagania w zakresie wsparcia technicznego i usług serwisowych zapewnianych przez Wykonawcę:
9.1. doradztwo telefoniczne oraz elektroniczne dotyczące korzystania z oprogramowania

9.2. usuwanie usterek, przez które rozumie się wszelkiego rodzaju nieprawidłowości w oprogramowaniu nie powodujące ograniczenia lub zakłócenia realizacji funkcji oprogramowania
9.3. serwis oprogramowania polegający na bezpłatnym dostępie do aktualizacji w okresie obowiązywania licencji
9.4. wsparcie techniczne do programu świadczone w języku polskim przez dystrybutora autoryzowanego przez producenta programu
9.5. wsparcie techniczne musi być dostępne przynajmniej od poniedziałku do piątku (w dni robocze) w godzinach od godziny: 8:00 – 15:30
9.6. czas reakcji na zgłoszenie – udzielenie odpowiedzi pozwalającej skutecznie wyeliminować napotkanego problemu związanego z eksploatacją systemu antywirusowego nie może być dłuższy niż 24h.

10. Wymagania w zakresie dokumentacji:

10.1. Wykonawca musi zapewnić dostęp do dokumentacji pozwalającej na samodzielne użytkowanie i administrowanie dostarczonym systemem antywirusowym
10.2. Dokumentacja musi być dostępna w polskiej wersji językowej
10.3. Udostępnienie dokumentacji może odbywać się na wskazanej przez Wykonawcę stronie internetowej