Załącznik Nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Główny kod CPV: 48761000-0 Pakiety oprogramowania antywirusowego

Przedmiotem niniejszego postępowania jest dostawa licencji oprogramowania ochrony antywirusowej i antyspamowej dla systemu teleinformatycznego Urzędu Miasta Łodzi wraz z asystą techniczną na okres 12 miesięcy (jednak nie wcześniej niż od 15 maja 2018r.). Licencja musi umożliwiać wykorzystanie oprogramowania na 4000 stacjach roboczych lub serwerach oraz 4500 użytkownikom serwera poczty elektronicznej (bramki smtp).

Termin wykonania zamówienia.
Wykonawca wykona zamówienie w niżej wymienionych etapach (jednak nie wcześniej niż od 15 maja 2018r.):
I etap – dostawa i wdrożenie oprogramowania do 22 dni roboczych od dnia wejścia w życie umowy,
II etap – asysta techniczna wdrożonego oprogramowania na okres 12 miesięcy od dnia wdrożenia i uruchomienia oprogramowania,

Oferowane rozwiązanie musi spełniać wymagania opisane w niniejszym opisie przedmiotu zamówienia w pkt. I. - „Wymagania minimalne dotyczące rozwiązania" oraz w pkt. II - „Wymagania minimalne dotyczące wdrożenia".
Zamawiający używa obecnie oprogramowanie Kaspersky Endpoint Security for Bussines Advanced – 3300 szt. licencji, oraz Kaspersky Secure Mail Gateway – 2800 szt. licencji z terminem wygaśnięcia 14 maja 2018 r.

I. Wymagania minimalne dotyczące rozwiązania

1. Wymagania ogólne

1.1 Rozwiązanie musi zapewnić ochronę w dwóch obszarach tj. ochronę stacji końcowej użytkownika i serwerów oraz ochronę poczty smtp (instalowane osobno, nie na działającym serwerze pocztowym).

1.2 Wszystkie moduły oprogramowania w każdym z obszarów opisanych w pkt. 1) muszą posiadać konsolę zarządzającą. Jedna konsola musi obejmować co najmniej funkcjonalność ochrony stacji końcowej użytkownika oraz serwerów. Zarządzanie systemem ochrony poczty smtp może być realizowane z wykorzystaniem konsoli dedykowanej lub poprzez konsolę do zarządzania ochroną stacji końcowej użytkownika oraz serwerów.

1.3 Zamawiający nie dopuszcza rozwiązań typu Unified Threat Managment (UTM).

1.4 W obszarze ochrony stacji końcowej użytkownika oraz serwerów, oprogramowanie musi realizować co najmniej następujące funkcjonalności:

ochrona antywirusowa, firewall, ids/ips na interfejsie sieciowym, kontrola aplikacji na stacjach roboczych i serwerach. Szczegółowy opis funkcjonalności jest opisany w pkt. 2. „Szczegółowe wymagania techniczne”.

1.5 W obszarze ochrony poczty smtp oprogramowanie musi realizować co najmniej następujące funkcjonalności: ochronę antywirusową i antyspamową. Szczegółowy opis funkcjonalności jest opisany w pkt. 2. „Szczegółowe wymagania techniczne”.

1.6 Pełna funkcjonalność klienta dla stacji roboczej musi być zawarta w jednym pliku instalacyjnym msi, zgodnym z Windows Installer.

1.7 Oprogramowanie musi działać na systemach Windows XP 32 bit z SP3, wszystkie wersje Windows: 7, 8.x,10 , Server 2008, Server 2008 R2, Server 2012, Server 2012 R2

1.8 Oferowane rozwiązanie musi poprawnie funkcjonować w zakresie serwerów zarządzających (konsola zarządzająca) oraz ochrony serwerów smtp w środowisku Microsoft Hyper-V 2012R2

1.9 Komponenty rozwiązania, które realizują funkcjonalności takie jak: firewall, zapobieganie włamaniom i kontrola aplikacji na stacjach roboczych, muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.

1.10 Serwer zarządzający musi działać na systemach Windows Server: 2008 R2, 2012, 2012R2.

1.11 Zarządzanie systemem ma być zapewnione poprzez graficzną konsolę administratora.

1.12 Rozwiązanie ma zapewniać wysoką skalowalność (obsługa min. 5 000 stacji).

1.13 Komunikacja pomiędzy agentami i serwerem ma być szyfrowana i kompresowana.

1.14 Numery portów używane do komunikacji mają mieć możliwość konfiguracji.

1.15 Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.

1.16 Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego źródła aktualizacji z możliwością konfiguracji określenia prędkości ich pobierania z serwera zarządzającego.

1.17 Jeżeli rozwiązanie wykorzystuje oprogramowanie firm trzecich, muszą zostać dostarczone wszelkie licencje na ich używanie.

1.18 Asysta techniczna świadczona przez producenta w swoim zakresie musi obejmować upgrade oprogramowania i jego składników, update definicji antywirusowych i antyspamowych oraz pomoc techniczną przy rozwiązywaniu

problemów z zaoferowanym oprogramowaniem. Czas naprawy nie dłuższy niż 14 dni.

2. Szczegółowe wymagania techniczne.

2.1 Ochrona antywirusowa stacji roboczej oraz serwerów:

2.1.1 Usuwanie wirusów, makro–wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu „spyware" i „adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez oprogramowanie tego typu;

2.1.2 Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym;

2.1.3 Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane;

2.1.4 Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych;

2.1.5 Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane: na dyskach twardych, w boot sektorach, na dyskietkach, na płytach CD/DVD, na zewnętrznych dyskach twardych (np. podłączonych przez port USB);

2.1.6 Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej;

2.1.7 Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta;

2.1.8 Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek;

2.1.9 Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych), w szczególności z plikach typu ZIP, GNU, LZH/LHA, BinHex, ARJ, RAR, MIME/UU, TAR, kontenery CAB, UUE, Rich Text Format;

2.1.10 Aktualizacja definicji wirusów nie wymagająca zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej;

2.1.11 Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące;

2.1.12 Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zestawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów;

2.1.13 Możliwość natychmiastowego „wypchnięcia” definicji wirusów do stacji klienckich;

2.1.14 Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 2 razy dziennie;

2.1.15 Możliwość aktualizacji bazy definicji wirusów średnio co 1 godzinę;

2.1.16 Heurystyczna technologia do wykrywania nowych, nieznanych wirusów;

2.1.17 Moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger;

2.1.18 Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe;

2.1.19 Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione;

2.1.20 Skanowanie poczty klienckiej (na komputerze klienckim);

2.1.21 Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach;

2.1.22 W wypadku systemu Windows 8 i 10, wsparcie dla funkcji ELAM (Early Launch Anti-Malware).

2.2 Firewall dla stacji roboczej oraz serwerów

2.2.1 Pełne zabezpieczenie stacji klienckich przed nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów;

2.2.2 Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe;

2.2.3 Administrator może definiować połączenia, które stacja robocza może inicjować
i odbierać;

2.2.4 Administrator może konfigurować dostęp stacji do następujących protokołów TCP, UDP, ICMP, IGMP

2.2.5 Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane jako: całkowicie bezpieczne lub niebezpieczne;

2.2.6 Program musi wykrywać próby wyszukiwania luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli;

2.2.7 Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: protokół sieciowy, stacja docelowa, aplikacja

2.2.8 Konfiguracja stacji ma się odbywać poprzez określenie: numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji dns (FQDN) lub domeny dns;

2.2.9 Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP;

2.2.10 Domyślne reguły zezwalające na ruch DHCP, DNS, WINS;

2.2.11 Wsparcie dla protokołu IPv6;

2.2.12 Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www – funkcjonalność opcjonalna, dodatkowo punktowana.

2.3 IDS/IPS na interfejsie sieciowym dla stacji roboczych i serwerów

2.3.1 Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą;

2.3.2 Wykrywanie skanowania portów;

2.3.3 Ochrona przed atakami typu odmowa usług (Denial of Service);

2.3.4 Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC);

2.3.5 Wykrywanie trojanów i generowanego przez nie ruchu;

2.3.6 Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie;

2.3.7 Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków;

2.4 Kontrola aplikacji na stacjach końcowych oraz serwerach

2.4.1 Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji;

2.4.2 Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową;

2.4.3 Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym;

2.4.4 Produkt ma kontrolować dostęp do rejestru systemowego;

2.4.5 Możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, aby żadna inna aplikacja/biblioteka spoza listy nie mogła uruchomić się na komputerze;

2.4.6 Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, aby tylko aplikacje znajdujące się na liście nie mogły uruchomić się na komputerze;

2.4.7 Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne – funkcjonalność opcjonalna, dodatkowo punktowana;

2.4.8 Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych – funkcjonalność opcjonalna, dodatkowo punktowana.

2.5 Szyfrowanie i deszyfrowanie na stacjach roboczych – funkcjonalność opcjonalna, dodatkowo punktowana.

2.5.1 Plików i katalogów

2.5.2 Całych dysków twardych

2.5.3 Przy użyciu algorytmu AES

2.5.4 Wszystkie działania związane z szyfrowaniem i deszyfrowaniem mają być całkowicie niewidoczne dla użytkownika

2.5.5 Mechanizm telefonicznego odzyskiwania hasła dla użytkownika znajdującego się poza siedzibą Zamawiającego

2.6 Centralna konsola zarządzająca dla stacji roboczych i serwerów

2.6.1 Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli;

2.6.2 Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci;

2.6.3 Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień;

2.6.4 Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami;

2.6.5 Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych;

2.6.6 Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze;

2.6.7 Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji;

2.6.8 Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu;

2.6.9 Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory.

2.6.10 Dostęp do interfejsu produktu dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej;

2.6.11 Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta;

2.6.12 Lokalizacja ma być określana według istnienia lub nieistnienia: adresu IP, zakresu podsieci, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS;

2.6.13 Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji;

2.6.14 W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu;

2.6.15 Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym;

2.6.16 Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej;

2.6.17 Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia: błędnej autoryzacji do systemu zarządzania, dostępności nowego oprogramowania, pojawienia się nowego komputera, zdarzeń powiązanych z infekcjami wirusów, stanu serwerów zarządzających;

2.6.18 Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.

2.6.19 Możliwość przejęcia stacji roboczej za pomocą konsoli administracyjnej.

2.7 Ochrona antywirusowa, antyspamowa oraz filtrowanie treści dla serwerów poczty smtp

2.7.1 licencja pozwalająca uruchomić zaoferowane rozwiązanie w środowisku wirtualnym Hyper-V;

2.7.2 Integracja z LDAP;

2.7.3 Zintegrowane rozwiązanie antywirusowe, antyspamowe i filtrowania treści;

2.7.4 Praca, jako bramka pocztowa;

2.7.5 Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowania na serwer usługodawcy;

2.7.6 Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 95%.

2.7.7 Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów lub dodanie wpisów na listach DNSBL i SURBL;

2.7.8 System ma zapewnić routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy;

2.7.9 System ma umożliwić zmianę domeny i nazwy użytkownika w wiadomości przychodzącej i wychodzącej dla odbiorcy i nadawcy odpowiednio dla ruchu przychodzącego i wychodzącego - funkcjonalnoć opcjonalna dodatkowo punktowana;

2.7.10 Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie się zawsze odbywać;

2.7.11 Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana;

2.7.12 Aktualizacje sygnatur spamu nie rzadziej, niż co 10 min;

2.7.13 Aktualizacje sygnatur antywirusowych nie rzadziej, niż co 2 godziny;

2.7.14 Skaner antywirusowy ma skanować skompresowane załączniki do 10 poziomów zagnieżdżeń w głąb i ma być odporna na złośliwie spreparowane załączniki („załączniki spakowane zawierające złośliwe oprogramowanie”);

2.7.15 Wiadomości z wirusami typu mass-mailer mają być w całości odrzucane, bez podejmowania dodatkowych akcji takich jak np. powiadomienie;

2.7.16 Wykrywanie fałszywych URL-i w wiadomościach;

2.7.17 Możliwość dodawania do odbieranych wiadomości zdefiniowanego tekstu;

2.7.18 Nakładanie polityk na załączniki w oparciu o ich rozmiar, typ MIME lub jego rozszerzenie;

2.7.19 Wiadomości sklasyfikowane jako spam można: usunąć/odrzucić, dodać nagłówek wiadomości, zarchiwizować, dostarczyć bez modyfikacji, usunąć załącznik z wiadomości;

2.7.20 Administrator ma mieć możliwość ingerencji w czułość rozwiązania;

2.7.21 Komunikacja w celu zarządzania systemem ma być szyfrowana;

2.7.22 Rozwiązanie ma być centralnie zarządzane z wbudowanymi mechanizmami raportowania;

2.7.23 System ma umożliwiać ustalenie co stało się z wiadomością;

2.7.24 System ma umożliwiać zapytanie o adres IP do globalnej bazy reputacji;

2.7.25 System musi umożliwiać skorzystania z predefiniowanych polityk i wzorców;

2.7.26 System musi wspierać autentykację SMTP;

2.7.27 Wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID – funkcjonalność opcjonalna, dodatkowo punktowana.

II. <u>Wymagania minimalne dotyczące wdrożenia.</u>

1. Czas wdrożenia nowego systemu antywirusowego musi zakończyć się najpóźniej w 22 dniu roboczym od daty wejścia w życie umowy, podczas którego muszą zostać wykonane wszystkie niżej wymienione zadania.

1.1 Wykonawca najpóźniej do 5 dnia roboczego od daty podpisania umowy przedstawi projekt wdrożenia nowego systemu.

1.2 Zamawiający w ciągu kolejnych 2 dni roboczych dokona przeglądu projektu wdrożenia i przedstawi swoje uwagi i komentarze.

1.3 Wykonawca w ciągu kolejnych 2 dni roboczych uwzględni uwagi Zamawiającego i przedstawi nową wersję projektu wdrożenia.

1.4 Wykonawca w ciągu kolejnych 10 dni, wdroży pełną funkcjonalność systemu antywirusowego i zgłosi gotowość do odbioru.

1.5 Zamawiający w ciągu kolejnych 3 dni roboczych dokona odbioru systemu.

2. Instalacja systemu antywirusowego wraz z agentami może rozpocząć się dopiero, po zaakceptowaniu przez Zamawiającego projektu wdrożenia.

3. Zakończenie wdrożenia systemu antywirusowego zostanie potwierdzone przez Zamawiającego i Wykonawcę poprzez podpisanie protokołu zdawczo-odbiorczego wdrożenia.

4. Wszystkie prace (poza wyszczególnionymi), które będą wykonywane u Zamawiającego muszą być realizowane w godzinach pracy Zamawiającego.

5. Wykonawca dokona analizy wykorzystywanego przez Zamawiającego systemu antywirusowego Kaspersky Endpoint Security for Bussines Advanced. Analiza musi obejmować minimum: architekturę funkcjonalną wdrożonego systemu, lokalizację wszystkich klientów oraz ich liczbę, systemy operacyjne, na których funkcjonują agenci. Analiza ta zostanie wykorzystana do odtworzenia wszystkich obecnie wdrożonych funkcjonalności i polityk bezpieczeństwa w zaoferowanym rozwiązaniu.

6. Wykonawca dokona deinstalacji obecnie wykorzystywanego systemu antywirusowego ochrony na wszystkich serwerach i wszystkich stacjach roboczych, o ile jest wymagana. W przypadku wystąpienia problemów podczas deinstalacji, ich rozwiązanie będzie należeć do Wykonawcy. Jednocześnie musi zostać zachowana pełna i prawidłowa funkcjonalność zainstalowanych innych aplikacji i systemów na danej stacji roboczej lub serwerze.

7. Wykonawca dokona instalacji agentów systemu antywirusowego na wszystkich stacjach roboczych podanych przez Zamawiającego. W przypadku wystąpienia problemów podczas instalacji, ich rozwiązanie będzie należeć do Wykonawcy. Jednocześnie musi zostać zachowana pełna i prawidłowa funkcjonalność zainstalowanych innych aplikacji i systemów na danej stacji roboczej .

8. Terminy instalacji agentów systemu na stacjach roboczych i serwerach muszą zostać uzgodnione z Zamawiającym i przedstawione w postaci harmonogramu w projekcie wdrożenia.

9. Wykonawca dokona instalacji agentów systemu na serwerach pod nadzorem osób wyznaczonych przez Zamawiającego. W przypadku wystąpienia

problemów podczas instalacji, ich rozwiązanie będzie należeć do Wykonawcy. Jednocześnie musi zostać zachowana pełna i prawidłowa funkcjonalność zainstalowanych innych aplikacji i systemów na danym serwerze.

10. Instalacje na serwerach wykonywane w godzinach pracy urzędu muszą zostać przeprowadzone w sposób, który nie zakłóca pracy użytkowników systemów pracujących na tych serwerach, w innym przypadku instalacja musi zostać przeprowadzona wyłącznie poza godzinami pracy.

11. W Urzędzie Miasta Łodzi stacje robocze zlokalizowane są w ok. 80 lokalizacjach na terenie miasta Łodzi. Lokalizacje w których sumaryczna ilość komputerów to ok. 2500 szt. podłączona jest siecią LAN o przepustowości min. 1Gbit/s, pozostałe to połączenia symetryczne 100Mbit/s oraz 2 połączenia 5Mbit/s (w sumie ok. 20-30 stacji roboczych).

12. Komputery podłączone są do Active Directory.

13. Obecnie wykorzystywane rozwiązanie musi funkcjonować do czasu pełnego wdrożenia zaoferowanego rozwiązania. W związku z tym, nie będzie możliwe wykorzystanie obecnie dedykowanych serwerów zarządzających dla nowego rozwiązania.

14. Zamawiający posiada infrastrukturę serwerową, która umożliwia uruchomienie w środowisku wirtualnym, 2 serwerów. Serwery mogą być utworzone na platformie Microsoft Hyper-v 2012R2 i środowisku zarządzającym SCVMM, każdy o następujących parametrach:

14.1 Maksymalna wielkość pamięci RAM - 12 GB.

14.2 Maksymalna wielkość przestrzeni dyskowej - 100 GB.

14.3 Maksymalna ilość VCPU – 2 szt.

15. Wykonawca przeprowadzi szkolenie dla min 10 osób w zakresie zarządzania systemem. Szkolenie musi zostać przeprowadzone zgodnie z zaleceniami dotyczącymi szkoleń, w zakresie czasu i tematyki zalecanej przez producenta zaoferowanego rozwiązania. Szkolenie musi być przeprowadzone nieodpłatnie na terenie miasta Łodzi lub poprzez Internet z aktywną komunikacją zarówno video jak i głosową z instruktorem prowadzącym szkolenie.

16. Wykonawca przygotuje dokumentację powykonawczą, która będzie obejmować, zawierającą w szczególności:

16.1 Analizę obecnie wykorzystywanego przez Zamawiającego systemu Kaspersky Endpoint Security for Bussines Advanced.

16.2 Architekturę wdrożonego systemu.

16.3 Wdrożone polityki.

16.4 Procedury backupu i odtwarzania

16.5 Opis konfiguracji bramki smtp.

16.6 Procedury rekonfiguracji bramki smtp.

16.7 Procedury restartu systemu.

17. W przypadku wypowiedzenia lub zerwania umowy w trakcie realizacji procesu wdrożenia, Wykonawca zobowiązany jest wykonać wszystkie czynności na własny koszt, które przywrócą środowisko informatyczne Zamawiającego do stanu przed rozpoczęciem procesu wdrożenia. W przypadku, gdy Wykonawca nie wykona tych czynności, Zamawiający wykona niezbędne prace z wykorzystaniem firm trzecich a kosztami tych prac obciąży Wykonawcę.

Termin wykonania zamówienia:
I etap – dostawa i wdrożenie oprogramowania do 22 dni roboczych od dnia wejścia w życie umowy (jednak nie wcześniej niż od 15 maja 2018 r.),
II etap – gwarancja i asysta techniczna wdrożonego oprogramowania na okres 12 miesięcy od dnia wdrożenia i uruchomienia oprogramowania.