Stanie się załącznikiem nr 1 do umowy

Opis Przedmiotu Zamówienia

Dostawa oprogramowania oraz wdrożenie systemu ochrony antywirusowej w środowisku sieci korporacyjnej statystyki publicznej

Przedmiotem zamówienia jest dostawa oprogramowania wraz z bezterminowymi licencjami i trzyletnim wsparciem producenta oraz wykonanie wdrożenia systemu antywirusowego **(rozumianego jako antymalware)** do ochrony infrastruktury posiadanej przez Zamawiającego w ośrodkach przetwarzania danych statystyki publicznej.

W szczególności przedmiot zamówienia obejmuje następujące zadania do realizacji przez Wykonawcę:

1. Dostawę oprogramowania antywirusowego wraz z bezterminowymi licencjami oraz trzyletnim wsparciem producenta na całe oprogramowanie wykorzystane do systemu ochrony antywirusowej,
2. Wdrożenie systemu antywirusowego w sieci korporacyjnej statystyki publicznej,
3. Przeprowadzenie szkoleń.

I. Wspólne uwarunkowania dla zadań oraz opis środowiska Zamawiającego

Prace wdrożeniowe i konfiguracyjne będą realizowane we wszystkich jednostkach statystyki publicznej, wyszczególnionych w poniższej tabeli, czyli w Podstawowym Centrum Przetwarzania Danych mieszczącym się w siedzibie Zamawiającego w Warszawie, w Zapasowym Centrum Przetwarzania Danych mieszczącym się w Zakładzie CIS w Radomiu, w 16 Urzędach Statystycznych a usługi dotyczą również 50 oddziałów terenowych Urzędów Statystycznych i Centrum Badań i Edukacji Statystycznej GUS w Jachrance . Wszystkie jednostki statystyki są połączone poprzez sieć WAN.

Lp.	Jednostki organizacyjne statystki publicznej	Adres
1.	Urząd Statystyczny w Białymstoku tel. 85 749 77 23	ul. Krakowska 13, 15-875 Białystok
2.	Urząd Statystyczny w Bydgoszczy tel. 52 366 93 85	ul. Konarskiego 1/3, 85-066 Bydgoszcz
3.	Urząd Statystyczny w Gdańsku tel. 58 768 31 84	ul. Danusi 4, 80-434 Gdańsk
4.	Urząd Statystyczny w Katowicach tel. 32 779 12 08	ul. Owocowa 3, 40-158 Katowice
5.	Urząd Statystyczny w Kielcach tel. 41 249 96 00	ul. Wróblewskiego 2, 25-369 Kielce
6.	Urząd Statystyczny w Krakowie tel. 12 361 01 65	ul. Kazimierza Wyki 3, 31-223 Kraków
7.	Urząd Statystyczny w Lublinie tel. 81 533 20 51	ul. Leszczyńskiego 48, 20-068 Lublin
8.	Urząd Statystyczny w Łodzi tel. 42 683 92 65	ul. Suwalska 29, 93-176 Łódź
9.	Urząd Statystyczny w Olsztynie tel. 89 524 36 34	ul. Kościuszki 78/82, 10-959 Olsztyn

Lp.	Jednostki organizacyjne statystki publicznej	Adres
10.	Urząd Statystyczny w Opolu tel. 77 423 01 10	ul. Kołłątaja , 45-064 Opole
11.	Urząd Statystyczny w Poznaniu tel. 61 279 83 30	ul. J.H. Dąbrowskiego 79, 60-529 Poznań
12.	Urząd Statystyczny w Rzeszowie tel. 17 853 52 19 w. 211	ul. Jana III Sobieskiego 10, 35-959 Rzeszów
13.	Urząd Statystyczny w Szczecinie tel. 91 459 77 10	ul. Matejki 22, 70-530 Szczecin
14.	Urząd Statystyczny w Warszawie tel. 22 464 22 54	ul. 1 Sierpnia 21, 02-134 Warszawa
15.	Urząd Statystyczny we Wrocławiu tel. 71 371 64 33	ul. Oławska 31, 50-950 Wrocław
16.	Urząd Statystyczny w Zielonej Górze tel. 68 322 31 21	ul. Spokojna 1, 65-954 Zielona Góra
17.	Centrum Informatyki Statystycznej Zakład w Radomiu tel. 48 362 42 17	ul. Planty 39/45, 26-600 Radom
18.	Główny Urząd Statystyczny (GUS) Centrum Informatyki Statystycznej (CIS) tel. 22 608 34 08	al. Niepodległości 208, 00-925 Warszawa

Z uwagi na fakt, iż prace wdrożeniowe i rekonfiguracyjne będą prowadzone na działającym środowisku sprzętowo–systemowo–aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska, minimalizacja przestojów, szczegółowe zaplanowanie wszelkich prac oraz przygotowanie scenariuszy awaryjnych.

1. Zamawiający korzysta z oprogramowania antywirusowego wraz ze wsparciem producenta ważnym do 31 grudnia 2017r, dostępnego w ramach pakietów:
    a. McAfee Endpoint Protection Suite,
    b. McAfee Move AV for Virtual Desktops,
    c. McAfee Move AV for Virtual Servers.
2. Zamawiający posiada domenę produkcyjną AD DS. Poziom funkcjonalny lasu i domeny ustawiony jest na Windows Server 2008 R2.
3. Na stacjach roboczych zainstalowane są systemy operacyjne MS Windows 8.1/10 odpowiednio w wersjach 32 i 64-bitowych.
4. Na serwerach zainstalowane są systemy operacyjne MS Windows Server 2008/2008R2/2012/2012R2/2016 odpowiednio w wersjach 32 i 64-bitowych.
5. Zamawiający wykorzystuje mechanizmy wirtualizacji do dostarczania wirtualnych desktopów i serwerów. Szczegółowy opis posiadanej infrastruktury znajduje się w punkcie ***Pojemność systemu docelowego.***

Opis infrastruktury sprzętowo-systemowej posiadanej przez Zamawiającego i dedykowanej dla wdrożenia systemu antywirusowego

1. Zamawiający udostępni do dyspozycji Wykonawcy możliwość tworzenia niezbędnej liczby maszyn wirtualnych wraz z licencjami serwerowymi MS Windows 2008 R2 lub 2012 R2, będącymi w posiadaniu Zamawiającego. Zamawiający dysponuje środowiskami do wirtualizacji serwerów:

    a. Zbudowanymi w oparciu o rozwiązania firmy Microsoft w Urzędach Statystycznych.

    b. VMware vCenter 5.1 w Podstawowym Centrum Przetwarzania Danych GUS w Warszawie oraz w Zapasowym Centrum Przetwarzania Danych w Radomiu.

2. Do utworzenia niezbędnych baz technicznych Zamawiający udostępni klaster MS SQL Server 2008 lub 2012.

3. Zamawiający posiada oprogramowanie antywirusowe:

    a. **1820** licencji McAfee Move AV for Virtual Desktops,

    b. **600** licencji McAfee Move AV for Virtual Servers,

    c. **6807** licencji McAfee Endpoint Protection .

W przypadku zaoferowania systemu, który nie będzie wykorzystywał udostępnionych przez Zamawiającego zasobów i posiadanych licencji, Wykonawca dostarczy wszystkie niezbędne elementy sprzętowe, systemowe i aplikacyjne.

II. Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę

Wykonawca przeprowadzi szczegółową analizę obecnie funkcjonującej infrastruktury systemu antywirusowego Zamawiającego przeznaczonej do uaktualnienia lub reinstalacji oraz opracuje i uzgodni z Zamawiającym koncepcję i harmonogram realizacji poszczególnych zadań.

Zadanie 1. Dostawa oprogramowania antywirusowego wraz z bezterminowymi licencjami oraz trzyletnim wsparciem producenta na całe oprogramowanie wykorzystane do systemu ochrony antywirusowej

Przedmiotem zadania jest dostawa oprogramowania antywirusowego wraz z bezterminowymi licencjami oraz trzyletnim wsparciem producenta pozwalającym na pobieranie aktualnych baz sygnatur wirusów, instalację nowych wersji oprogramowania i korzystanie z pomocy technicznej.

Wymagania Zamawiającego

Wymagania ogólne w zakresie licencji

1. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi i serwerami (np. w przypadku wymiany sprzętu) oraz możliwość sublicencjonowania dla jednostek organizacyjnych służb statystyki publicznej podległych Prezesowi GUS.

2. Zamawiający oczekuje aktywacji kluczy wsparcia producenta nie wcześniej niż od 1 stycznia 2018 r.

3. Zamawiający wymaga trzyletniego wsparcia producenta na zamawiane oprogramowanie.

Pojemność systemu docelowego

Licencje mogą być dostarczone w pakiecie zawierającym różne funkcjonalności lub jako samodzielne produkty, ale muszą pochodzić od tego samego producenta oprogramowania antywirusowego. Zamawiający wymaga dostarczenia nowego oprogramowania lub uzupełnienia oprogramowania posiadanego przez Zamawiającego wraz z wykupieniem usługi wsparcia producenta dla oprogramowania dostarczanego oraz posiadanego przez Zamawiającego, jeśli będzie wykorzystywane, do ochrony następującej liczby i typów obiektów:

1. **7800** fizycznych stacji roboczych z systemem MS Windows 8.1/10 oraz serwerów w systemem operacyjnym MS Windows Server 2008/2008 R2/2012/2012 R2/2016.
2. **1820** wirtualnych stacji z systemem MS Windows 7 udostępnianych poprzez oprogramowanie VMwareView 5.2 wraz z VMware vCenter 5.0 lub 5.1.
3. **300** wirtualnych serwerów (wersja systemu jak w pkt. 1) korzystających z infrastruktury wirtualizacji Microsoft.
4. **300** wirtualnych serwerów (wersja systemu jak w pkt. 1) korzystających z infrastruktury VMware vCenter 5.1 oraz 5.5.

Podstawowe wymagania funkcjonalne

Oferowane rozwiązanie musi pochodzić od jednego producenta. Zintegrowany system ochrony dla stacji roboczych i serwerów, powinien posiadać następujące moduły funkcjonalne:

1. Centralny system instalacji i zarządzania wszystkimi modułami wchodzącymi w skład systemu antywirusowego z wykorzystaniem jednej konsoli zarządzającej, która odpowiada także za centralne gromadzenie zdarzeń (logów) z poszczególnych modułów oraz przetwarzanie ich do postaci raportów.
2. Moduł ochrony działający w czasie rzeczywistym chroniący przed oprogramowaniem typu: wirusy, trojany, robaki, adware, spyware i innym potencjalnie złośliwym kodem poprzez wykrywanie, usuwanie lub blokowanie wykrytego szkodliwego oprogramowania dla stacji roboczych i serwerów.
3. Moduł ochrony przed szkodliwym oprogramowaniem dedykowany do zabezpieczania środowisk wirtualnych, w których pracują wirtualne serwery i desktopy.
4. Moduł kontroli wykorzystania portów i urządzeń podłączanych do fizycznych stacji roboczych (co najmniej porty USB, szeregowe, adaptery Bluetooth) umożliwiający blokowanie portów i nieautoryzowanych urządzeń, powiadamianie użytkownika o wykryciu naruszenia polityki, przekazywanie alertów o incydentach do centralnej konsoli.
5. Moduł automatycznego wykrywania w sieci nowych, pozbawionych ochrony antywirusowej komputerów i urządzeń sieciowych wysyłający raporty do centralnej konsoli zarządzania.

Szczegółowe wymagania funkcjonalne dotyczące najważniejszych modułów /elementów systemu antywirusowego

1. **Centralny system instalacji i zarządzania (centralna konsola zarządzania) musi posiadać poniższe cechy:**
    a. Zarządzanie wszystkimi modułami i pełnym zakresem funkcji dostarczonego systemu ochrony antywirusowej powinno następować z jednej i tej samej aplikacji działającej na serwerze z systemem operacyjnym MS Windows Server 2008 R2 lub nowszym, korzystającej z bazy danych MS SQL.

b. Aplikacja ma umożliwiać tworzenie hierarchii serwerów zarządzających, co umożliwi: hierarchiczne definiowanie polityk działania produktów – wymuszanie ustawień konfiguracyjnych z głównego serwera zarządzania do serwerów niższego poziomu oraz automatyczne przekazywanie wybranych logów i zdarzeń z serwerów niższego poziomu do serwera centralnego w celu kompleksowego raportowania stanu zabezpieczeń.
c. Wdrożenie dowolnej liczby dodatkowych serwerów zarządzania zarówno pracujących niezależnie od siebie, jak również w układzie hierarchicznym, nie może wymagać zakupu dodatkowych licencji lub oprogramowania.
d. System musi umożliwiać migrację zarządzanych komputerów między serwerami zarządzania (zmiana przypisania komputera do konkretnego serwera zarządzania).
e. System powinien mieć możliwość działania w klastrze HA.
f. Konsola ma umożliwić zdalną instalację produktów na komputerach z domeny AD DS bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów.
g. Oferowane rozwiązanie ma umożliwiać selektywne wskazanie, który z produktów wchodzących w skład systemu antywirusowego zostanie wdrożony. Nie jest dopuszczalne wdrożenie pakietu w postaci jednej paczki instalacyjnej obejmującej kilka produktów.
h. Definiowanie komputerów, które mają być objęte wdrożeniem poszczególnych produktów musi być możliwe na podstawie zdefiniowanych grup maszyn oraz na bazie dynamicznie przydzielanych znaczników, niezależnie od przynależności do grupy maszyn.
i. Zarządzanie powinno odbywać się poprzez standardową przeglądarkę WWW i połączenie https.
j. Komunikacja wszystkich produktów wdrożonych na danym komputerze musi odbywać się okresowo poprzez jeden kanał komunikacji.
k. Musi być możliwe wymuszenie połączenia komputera z serwerem zarządzania na żądanie ze strony konsoli.
l. Konsola musi umożliwiać tworzenie szczegółowych konfiguracji działania poszczególnych produktów, dystrybucję polityk oraz wymuszanie ich zastosowania.
m. Konsola ma umożliwiać przydzielenie różnych polityk do poszczególnych komputerów, grup maszyn oraz dynamicznie (niezależnie od przydziału do grupy) na podstawie filtrów bazujących na parametrach sprzętowych lub systemowych.
n. Musi być dostępna funkcjonalność wymuszania, w zdefiniowanym przedziale czasu, przywrócenia ustawień konfiguracji w przypadku, gdy użytkownik zmodyfikuje ustawienia.
o. Konsola musi posiadać funkcjonalność powiadamiania o zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP lub wywołania komendy/skryptu.
p. Konsola powinna posiadać możliwość integracji z AD DS zarówno w rozumieniu powielenia struktury komputerów, jak również autentykacji i autoryzacji administratorów.
q. Konsola ma umożliwiać zdefiniowanie wielu kont administratorów i przydzielenie im szczegółowych ról umożliwiających co najmniej: ograniczenie dostępu do wskazanych grup maszyn, ograniczenie administracji do poszczególnych produktów i ich specyficznych funkcji.

r. Konsola ma zapewnić centralne repozytorium dla logów i zdarzeń logowanych przez wszystkie moduły systemu ochrony antywirusowej.

s. Aplikacja zarządzająca ma umożliwiać centralne opracowanie raportów na podstawie zgromadzonych danych i prezentację ich w różnych formatach (co najmniej PDF, XML, HTML).

2. System ochrony działający na stacjach roboczych i serwerach musi spełniać poniższe wymagania:

a. Oprogramowanie ma zapewnić wsparcie dla platformy systemowej MS Windows odpowiednio w wersjach 32 i 64-bitowej: MS Windows 8.1/10 oraz MS Windows Server 2008/2008R2/2012/2012R2/2016.

b. Dodatkowo w ramach oferowanego pakietu musi być dostępne narzędzie do skanowania plików, uruchamiane z linii komend (CLI).

c. System ma zapewniać przyrostowe aktualizacje baz sygnatur dla chronionych komputerów z centralnego serwera zarządzania oraz serwerów FTP, HTTP, UNC.

d. System ochrony na komputerach ma mieć możliwość pracy bez bezpośredniego połączenia z siecią Internet.

e. Musi być zapewniona możliwość ręcznej aktualizacji produktów i baz sygnatur.

f. System ma zapewnić ochronę antywirusową na podstawie:

   i. sygnatur,

   ii. heurystyki (z możliwością jej wyłączenia),

   iii. na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet.

g. Skanowanie antywirusowe ma się odbywać w chwili dostępu, na żądanie i według harmonogramu.

h. Skanowanie na żądanie i wg harmonogramu musi mieć możliwość przerwania w dowolnym momencie (np. wykrycia pracy na baterii).

i. Moduł ochrony ma mieć możliwość określania różnych konfiguracji skanowania dla różnych procesów (np. ftp – wysokie, backup niskie) oraz definiowania wykluczeń skanowania określonych zasobów.

j. Moduł ochrony ma zapewniać ochronę przed wykorzystaniem luk bezpieczeństwa.

k. System ma zapewnić skanowanie pamięci operacyjnej i rejestru komputera.

l. System ma zapewnić moduł antyspyware działający w czasie rzeczywistym.

m. System musi umożliwiać definiowanie reguł pozwalających na blokowanie dostępu do określonych zasobów.

n. System powinien posiadać ochronę serwisów oprogramowania antywirusowego zabezpieczającą przed zatrzymaniem (nawet z konta z uprawnieniami lokalnego administratora).

o. System powinien posiadać możliwość ograniczenia opcji konfiguracyjnych modułów ochronnych lub zabezpieczenia ich hasłem.

p. Musi istnieć możliwość automatycznego zainstalowania na komputerach nowych silników antywirusowych, poprawek do produktów oraz hotfixów z centralnego serwera zarządzającego lub lokalnych repozytoriów.

q. System musi być kompatybilny z usługą MS Direct Access.

3. **Moduł ochrony przed złośliwym oprogramowaniem dedykowany do zabezpieczania środowisk wirtualnych musi spełniać wymagania:**
    a. Oprogramowanie musi chronić przed szkodliwym oprogramowaniem wirtualne desktopy i serwery w trakcie ich pracy.
    b. Oprogramowanie powinno umożliwiać skanowanie bezagentowe (tylko z użyciem agenta VMware) oraz agentowe (niezależne od platformy wirtualizacyjnej).
    c. Przy skanowaniu bezagentowym oprogramowanie musi mieć możliwość definicji polityk skanowania z dokładnością do jednej maszyny wirtualnej.
    d. Oprogramowanie powinno umożliwiać sprawdzenie reputacji skanowanych plików w centralnej bazie dostępnej w Internecie.
    e. Oprogramowanie powinno umożliwiać użycie kwarantanny dla zainfekowanych plików.
    f. Oprogramowanie działające w trybie skanowania agentowego i bezagentowego musi być zarządzane z jednej centralnej konsoli zarządzającej.
    g. Przy skanowaniu agentowym oprogramowanie musi umożliwiać skanowanie wirtualnych maszyn na żądanie.
    h. Oprogramowanie musi posiadać funkcjonalność wykrywania obciążania procesora hypervisora.

4. **Moduł kontroli portów i podłączanych urządzeń do stacji użytkowników musi posiadać poniższe cechy:**
    a. Modułu kontroli portów musi wspierać instalacje na systemach operacyjnych: MS Windows 7/8.1/10.
    b. Moduł musi w sposób minimalny wpływać na obciążenie hosta oraz powinna istnieć możliwość ograniczenia ilości zajmowanej pamięci RAM.
    c. Moduł musi wykrywać i blokować urządzenia podłączane przez porty zewnętrzne komputera (wliczając w to: USB, porty szeregowe), takie jak: dyski zewnętrzne, pendrive, MTP, PDA, kamera cyfrowa, odtwarzacze MP3, drukarki i inne typy urządzeń oraz umożliwiać zmianę sposobu dostępu do urządzeń posiadających system plików na tryb „tylko do odczytu”.
    d. Rozwiązanie musi przechowywać informacje o nazwie urządzenia, czasie przyłączenia, typie urządzania, kodzie producenta i urządzenia oraz numerze seryjnym.
    e. Konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania nośników danych USB na podstawie ich numeru seryjnego, ID producenta i produktu.
    f. Polityka działania modułu musi umożliwiać przypisanie różnych parametrów zależnie od poszczególnych użytkowników, grup użytkowników synchronizowanych z AD DS oraz grup komputerów.
    g. Oprogramowanie musi być zarządzane z centralnej konsoli zarządzającej.

Zadanie 2. Wdrożenie systemu antywirusowego w sieci korporacyjnej statystyki publicznej

Przedmiotem zadania jest wdrożenie system ochrony antywirusowej w oparciu o dostarczone oprogramowanie w infrastrukturze posiadanej przez Zamawiającego w ośrodkach przetwarzania danych statystyki publicznej.

Wymagania projektowe

1. W trakcie trwania wdrożenia środowisko Zamawiającego musi być objęte nieprzerwanie ochrona antywirusową.
2. Usługi systemu antywirusowego muszą być dostępne we wszystkich lokalizacjach włączonych do sieci korporacyjnej.
3. System antywirusowy powinien być zintegrowany z posiadanymi przez Zamawiającego usługami katalogowymi AD DS.
4. Administrowanie infrastrukturą powinno być scentralizowane z możliwością delegowania poszczególnych uprawnień do poziomu jednostek organizacyjnych GUS, CIS i Urzędów Statystycznych (18 lokalizacji głównych).
5. Administratorzy systemu powinni mieć możliwość nadzorowania i sprawnego zarządzania całym systemem.

Szczegółowa specyfikacja prac

W ramach przedmiotu umowy Wykonawca wykona następujące prace:

1. Przygotuje optymalny **Projekt techniczny** realizacji uzgodnionej koncepcji uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta oprogramowania.
2. Przygotuje koncepcję realizacji zadania.
3. Opracuje i uzgodni szczegółowy harmonogram realizacji prac uwzględniający specyfikę organizacji Zamawiającego.
4. Przeprowadzi wdrożenie pilotażowe i uzyska akceptację Zamawiającego.
5. Wdroży i skonfiguruje w jednostkach statystyki publicznej oprogramowanie według zaakceptowanego Projektu technicznego w oparciu o najnowsze, rekomendowane przez producenta wersje produktów w tym m.in.:
    a. ochronę stacji roboczych i serwerów, w tym stacji mobilnych i środowisk chronionych,
    b. ochronę środowisk wirtualnych,
    c. kontrolę portów stacji roboczych,
    d. wykrywanie w sieci nowych komputerów i urządzeń.
6. Dokona migracji lub wymiany komponentów obecnego używanego systemu antywirusowego Zamawiającego.
7. Skonfiguruje polityki konfiguracyjne z wykorzystaniem najlepszych praktyk producenta oprogramowania dla wdrożonych modułów i produktów.
8. Skonfiguruje profile skanowania podczas dostępu zawierające m.in. proponowane elementy skanowania, wykluczenia oraz kategoryzację procesów dla poszczególnych typów serwerów, stacji roboczych i aplikacji w oparciu o rekomendowane pod kątem bezpieczeństwa i wydajności rozwiązania producenta oprogramowania m.in. dla:
    a. Kontrolerów domeny, klastrów failover, hostów Hyper-V, serwerów SQL, SCOM, IIS, SharePoint, Tomcat, Apache, Java, Citrix, Exchange, backup.
    b. Stacjonarnych i mobilnych stacji roboczych.
    c. Wirtualnych stacji roboczych i serwerów.
9. Skonfiguruje zadania skanowania na żądanie dla obiektów wyszczególnionych w pkt. 8.

10. Skonfiguruje uzgodnione z Zamawiającym dodatkowe, niestandardowe raporty w centralnej konsoli zarządzania.
11. Skonfiguruje uzgodnione z Zamawiającym ustawienia i zestawy polityki w module kontroli portów.
12. Opracuje scenariusze testowe i przeprowadzi testy akceptacyjne wdrożonego rozwiązania.
13. Opracuje i przedstawi Raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy.
14. Wykonawca opracuje **Dokumentację powykonawczą**, która będzie zawierać:
    a. Opis architektury zaimplementowanego rozwiązania.
    b. Szczegółowy opis instalacji i konfiguracji wykorzystywanego oprogramowania, ze wskazaniem wybranych opcji i ustawionych wartości.
    c. Konfigurację poszczególnych serwerów, modułów, komponentów i usług.
    d. Zbiór zaimplementowanych polityk konfiguracyjnych dla poszczególnych produktów i modułów.
    e. Zbiór zaimplementowanych wykluczeń skanowania dla poszczególnych typów serwerów, stacji roboczych i aplikacji zawierający rekomendowane pod kątem bezpieczeństwa i wydajności rozwiązania producenta oprogramowania.
    f. Zbiór przygotowanych zadań skanowania na żądanie dla poszczególnych typów serwerów i stacji roboczych.
    g. Politykę i procedury wykonywania kopii zapasowych.
    h. Szczegółowe procedury eksploatacyjne oraz awaryjnego odtwarzania funkcjonalności systemu, opisujące krok po kroku niezbędne czynności umożliwiające Zamawiającemu samodzielne przywrócenie funkcjonalności systemu.
    i. Procedury i instrukcje bieżącego monitoringu oraz utrzymania i aktualizacji systemu.

    Zamawiający wymaga, aby Dokumentacja powykonawcza napisana była w języku polskim. Wykonawca przekaże Zamawiającemu Dokumentację powykonawczą w trzech egzemplarzach w formie papierowej oraz w formie elektronicznej na nośniku CD. Dokumentacja na nośniku CD musi posiadać format pliku do edycji.

Zadanie 3. Przeprowadzenie szkoleń

1. Wykonawca przeprowadzi szkolenia zgodnie z następującymi wymaganiami:
    a. **Szkolenie dla administratorów systemu ochrony antywirusowej**
        i. dwie grupy uczestników po 19 osób, (uczestnicy z lokalizacji wymienionych w tabeli w pkt.1),
        ii. czas trwania szkolenia: 3 dni robocze (24 godziny zegarowe),
    b. program szkolenia – instalacja i konfiguracja komponentów wdrożonego rozwiązania ze szczególnym uwzględnienie konfiguracji centralnej konsoli zarządzania, środowisk wirtualnych oraz programu do kontroli portów.
    c. wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF.
    d. wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia i posiadania odpowiednich kompetencji administratora.

e. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

f. Wykonawca pokryje wszelkie koszty związane z pobytem na szkoleniu czyli wyżywieniem i zakwaterowaniem uczestników w pokojach 2 lub 1 osobowych.

g. Wykonawca zapewni nocleg uczestnikom szkolenia na dzień przed planowaną datą rozpoczęcia szkolenia.

h. Wykonawca zapewni transport z miejsca zakwaterowania do miejsca szkolenia.

i. Wymagania szczegółowe dla szkolenia:

   i. musi mieć formę wykładów i warsztatów,
   ii. Wykonawca każdego dnia trwania szkolenia zapewni: dwie przerwy kawowe, każda trwająca ok. 10 minut oraz jedną przerwę obiadową trwającą ok. 40 minut.
   iii. Wykonawca zapewni każdego dnia szkolenia wyżywienie dla wszystkich uczestników:
      a) dostępne przez cały czas trwania szkolenia: kawa, herbata, butelkowana woda mineralna gazowana i niegazowana, naturalne soki owocowe (butelkowane lub w kartonach) oraz ciastka.
      b) obiad – zupa, danie główne, surówki, owoce, herbata, kawa, butelkowana woda mineralna, naturalne soki owocowe (butelkowane lub w kartonach); czyste sztućce i zastawa (nie mogą być jednokrotnego użytku) – podany w oddzielnym pomieszczeniu (strefie przeznaczonej do podawania posiłków):

2. 20 dni od daty podpisania Umowy Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkoleń przygotowany w porozumieniu z Zamawiającym obejmujący:
   a. program szkoleń zawierający szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć,
   b. metodę prowadzenia szkoleń,
   c. listę wykładowców i informacje o wykładowcach, którzy przeprowadzą poszczególne szkolenia.
3. Wykonawca zobowiązany będzie do przeprowadzenia szkoleń zgodnie z zatwierdzonym przez zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkoleń.
4. Zamawiający zastrzega sobie prawo do modyfikacji harmonogramu szkoleń, z wytypowaniem na poszczególne cykle mniejszej lub większej liczby uczestników, z zachowaniem ilości cykli szkoleń i sumarycznej liczby uczestników.
5. Wykonawca w ramach prowadzonych szkoleń zobowiązany jest zapewnić:
   a. materiały szkoleniowe dla każdego uczestnika szkolenia,
   b. wydanie imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenie, pod warunkiem uczestnictwa w pełnym wymiarze zajęć.
6. Wykonawca przekaże Zamawiającemu listy obecności podpisane przez uczestników szkoleń.