CZĘŚĆ 4 Załącznik nr 1.4

Dostawa licencji na oprogramowanie biurowe (34 szt.) i antywirusowe (35 szt.)

Formularz ofertowy – Załącznik nr 1.4 SWZ

SZCZEGÓŁOWA SPECYFIKACJA TECHNICZNA

4.1 Dostawa licencji na oprogramowanie pakietu biurowego w wersji edukacyjnej (akademickiej) – łącznie 34 szt.

Wstęp

Zamawiający obecnie posiada i eksploatuje następujące licencje pakietów biurowych typu ACADEMIC:

- 63 licencje na oprogramowanie Microsoft Office Professional Plus 2019 PL (najnowsza wersja),
- ponad 110 licencji na oprogramowanie Microsoft Office Professional Plus 2016 PL,
- 190 licencji na oprogramowanie Microsoft Office Professional Plus 2013 PL,
- 190 licencji na oprogramowanie Microsoft Office Professional Plus 2010 PL,
- ponad 210 licencji na oprogramowanie Microsoft Office Professional Plus 2007 PL

zainstalowanych na sprzęcie komputerowym wyposażonym w system operacyjny **Microsoft Windows 7, 8, 8.1, 10.**

Zamawiający posiada także wdrożony **zintegrowany system finansowo-księgowy** (oprogramowanie **Simple.ERP**), który jest ściśle **zintegrowany** z oryginalnymi bibliotekami i sterownikami zawartymi w pakiecie oprogramowania Microsoft Office (różnych jego wersji), z wykorzystaniem których tworzone są różnego rodzaju zestawienia, wykresy, wydruki, itd.

Opis przedmiotu zamówienia:

Dostawa licencji <u>akademickich</u> na oprogramowanie profesjonalnego pakietu biurowego – 34 szt. (z 1 kpl. nośników).

Przedmiotem zamówienia jest dostawa **bezterminowych** licencji na oprogramowanie **profesjonalnego pakietu biurowego (wyprodukowanego przez jednego producenta), o minimalnej funkcjonalności przedstawionej poniżej, w wersji polskiej, aktualnej na rok 2021 tj. najnowszej stabilnej, opublikowanej przez producenta, akademickiej (typu EDU lub ACADEMIC) – przeznaczonej dla jednostek naukowych i edukacyjnych,** w pełni kompatybilne na poziomie **obsługiwanych formatów, wymiany plików oraz bibliotek i sterowników** z wymienionym we Wstępie oprogramowaniem użytkowanym obecnie u Zamawiającego oraz systemem operacyjnym **Microsoft Windows 10** zainstalowanym na dysponowanym obecnie przez Zamawiającego sprzęcie komputerowym.

Wszystkie oferowane Licencje i Oprogramowanie muszą być fabrycznie nowe, nigdy wcześniej nie aktywowane, wszystkie skojarzone z tym samym kluczem aktywacyjnym (lub równoważnym identyfikatorem aktywacyjnym) oraz muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta obejmujących rynek polski, zapewniających w szczególności realizację uprawnień gwarancyjnych.

Przedmiotem zamówienia jest zatem **rozszerzenie o 34 szt. licencji na najnowszą wersję oprogramowania pakietu biurowego posiadanego przez Zamawiającego** lub dostawa **34 szt.** licencji na **rozwiązanie równoważne** zgodnie z warunkami przedstawionymi poniżej. Licencje na pakiet oferowanego oprogramowania biurowego muszą być dostarczone w opcji przysługującej jednostkom akademickim (wersja EDU, ACADEMIC).

UWAGA: Ww. licencje muszą zostać dostarczone Zamawiającemu przez Wykonawcę **bez konieczności zawierania przez Zamawiającego żadnych dodatkowych umów** z wyjątkiem umowy kupna-sprzedaży pomiędzy Zamawiającym i Wykonawcą, której wzór zawarty jest w SWZ.

Warunki równoważności na pakiet profesjonalnego oprogramowania biurowego

Zamawiający uzna, że zaoferowany pakiet oprogramowania biurowego jest zgodny z przedmiotem zamówienia jeżeli będzie on zawierał funkcjonalności **co najmniej tożsame lub lepsze** od określonych w niniejszym opisie przedmiotu zamówienia w zakresie posiadanej funkcjonalności i będzie kompatybilny w 100% z oprogramowaniem posiadanym przez Zamawiającego, o którym mowa we Wstępie do niniejszego opisu przedmiotu zamówienia.

W przypadku zaproponowania wersji równoważnej Wykonawca **zobowiązany jest załączyć do oferty opis (karty katalogowe) i dane techniczne** zaproponowanego rozwiązania umożliwiające porównanie go ze wszystkimi parametrami wymaganymi niniejszym opisem przedmiotu zamówienia w tym **zgodność ww. oprogramowania posiadanego przez Zamawiającego** z zaproponowanym rozwiązaniem.

Przez wykazanie równoważności Zamawiający rozumie wykonanie stosownych porównań i analiz przez Wykonawcę. **Wyniki porównań i analiz w formie tabelarycznej należy załączyć do oferty.**

Zamawiający zastrzega sobie prawo do **zweryfikowania funkcjonalności, wydajności i kompatybilności** zaoferowanego rozwiązania równoważnego poprzez analizę jego funkcjonalności oraz **praktyczne zbadanie możliwości jego współpracy z posiadanym systemem finansowo-księgowym SIMPLE.ERP a także możliwości przetwarzania z wykorzystaniem zaoferowanego rozwiązania plików Zamawiającego wytworzonych za pomocą posiadanego wymienionego we Wstępie oprogramowania**. Produkty oferowanego rozwiązania równoważnego muszą być również w pełni kompatybilne z posiadanym przez Zamawiającego oprogramowaniem **bez potrzeby dodatkowej edycji, formatowania, konwertowania i modyfikowania**.

W przypadku skorzystania przez Zamawiającego z ww. uprawnienia Wykonawca jest zobowiązany w terminie 3 dni od dnia otrzymania od Zamawiającego wezwania do dostarczenia testowej wersji zaproponowanego rozwiązania, dostarczyć to rozwiązanie do siedziby Zamawiającego.

Dostarczany pakiet oprogramowania biurowego musi posiadać następujące, wbudowane funkcjonalności:

1. Posiadać pełną polską wersję językową interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na język angielski wraz z dostępną pełną dokumentacją w języku polskim
2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   - posiada kompletny i publicznie dostępny opis formatu,
   - ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. 2017 poz. 2247),
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców,

4. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
5. Możliwość dostosowania dokumentów i szablonów do potrzeb Zamawiającego oraz udostępnienie narzędzi umożliwiających dystrybucję odpowiednich szablonów do właściwych odbiorców.
6. Narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy – zgodny z posiadanym przez Zamawiającego Visual Basic for Application).
7. Pakiet musi zawierać następujące aplikacje wyprodukowane przez jednego producenta:
    a. edytor tekstów,
    b. arkusz kalkulacyjny,
    c. narzędzie do przygotowywania i prowadzenia prezentacji,
    d. narzędzie do tworzenia i pracy z lokalną bazą danych,
    e. narzędzie do tworzenia i wypełniania formularzy elektronicznych,
    f. narzędzie do tworzenia drukowanych materiałów informacyjnych,
    g. narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
    h. narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR,
    i. narzędzie do prowadzenia spotkań internetowych on-line (wideokonferencji),
    j. dostęp do dedykowanej chmury producenta oprogramowania.

8. Edytor tekstów umożliwiający co najmniej:

    Edycję i formatowanie tekstu w języku polskim i angielskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty; wstawianie oraz formatowanie tabel; wstawianie oraz formatowanie obiektów graficznych; wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne); automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków; automatyczne tworzenie spisów treści; przypisów i spisów literatury; formatowanie nagłówków i stopek stron; sprawdzanie pisowni w języku co najmniej polskim i angielskim; formatowanie rysunków: przycinanie, definiowanie położenia, wielkości i współczynnika kształtu i opływania tekstu; śledzenie zmian wprowadzonych przez użytkowników; komentowanie tekstów i zarządzanie zmianami w dokumentach, w tym definiowanie sposobu graficznej prezentacji zmian; nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności; określenie układu strony (pionowa/pozioma); wydruk dokumentów; wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną; pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word w wersjach 2007, 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu; zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji; ustawianie jedno i wielostronicowych widoków dokumentu; wsparcie statystyki wyrazów i znaków w dokumencie; automatyczne konwertowanie dokumentów do formatu pdf, xml i html;

9. Arkusz kalkulacyjny umożliwiający co najmniej:

Tworzenie raportów tabelarycznych; tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych, warstwowych, XY, kolumnowych, powierzchniowych; tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu; tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice); obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych; tworzenie raportów tabel przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabel przestawnych; wyszukiwanie i zamianę danych; wykonywanie analiz danych przy użyciu formatowania warunkowego; nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie; nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności; formatowanie czasu, daty i wartości finansowych z polskim formatem; zapis wielu arkuszy kalkulacyjnych w jednym pliku; zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania posiadanego przez Zamawiającego oprogramowania Microsoft Excel w wersjach 2007, 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń; zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

10. Narzędzie do przygotowywania i prowadzenia prezentacji umożliwiające:

Przygotowywanie prezentacji multimedialnych, które będą: prezentowane przy użyciu projektora multimedialnego; drukowane w formacie umożliwiającym robienie notatek; zapisane jako prezentacja tylko do odczytu; nagrywanie narracji i dołączanie jej do prezentacji; opatrywanie slajdów notatkami dla prezentera; umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo; umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego; odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym; możliwość tworzenia animacji obiektów i całych slajdów; automatyczne nakładanie predefiniowanych szablonów na stworzone gotowe prezentacje; prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft PowerPoint w wersjach 2007, 2010, 2013, 2016 i 2019.

11. Zintegrowane z pakietem narzędzie do zarządzania informacją prywatną umożliwiające:

Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego; filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców; tworzenie katalogów, pozwalających katalogować pocztę elektroniczną; tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy; oflagowanie poczty elektronicznej z określeniem terminu przypomnienia; zarządzanie kalendarzem; udostępnianie kalendarza innym użytkownikom; przeglądanie kalendarza innych użytkowników; zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach; zarządzanie listą zadań; zlecanie zadań innym użytkownikom; zarządzanie listą kontaktów; udostępnianie listy kontaktów innym użytkownikom; przeglądanie listy kontaktów innych użytkowników; możliwość przesyłania kontaktów innym użytkownikom.

12. Narzędzie do tworzenia i pracy z lokalną bazą danych umożliwiające:

Tworzenie bazy danych przez zdefiniowanie: tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych; relacji pomiędzy tabelami; formularzy do wprowadzania i edycji danych; raportów; edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych; tworzenie bazy danych przy użyciu zdefiniowanych szablonów; połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym; pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Access w wersjach 2007, 2010, 2013, 2016 i 2019, niezbędna do pracy na posiadanych plikach już utworzonych z pomocą ww. oprogramowania posiadanego i wykorzystywanego przez Zamawiającego.

13. Narzędzie do tworzenia drukowanych materiałów informacyjnych umożliwiające:

Tworzenie i edycję drukowanych materiałów informacyjnych; tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów; edycję poszczególnych stron materiałów; podział treści na kolumny; umieszczanie elementów graficznych; wykorzystanie mechanizmu korespondencji seryjnej; płynne przesuwanie elementów po całej stronie publikacji; eksport publikacji do formatu PDF oraz TIFF; wydruk publikacji; możliwość przygotowywania materiałów do wydruku w standardzie CMYK

14. Narzędzie do tworzenia formularzy elektronicznych umożliwiające:

Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania; umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków; utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników; pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych; możliwość pobierania danych z platformy do pracy grupowej; przesłanie danych przy użyciu usługi Web (tzw. webservice); wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML; podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.

Ponadto dostarczany pakiet oprogramowania biurowego musi zawierać biblioteki i sterowniki w pełni kompatybilne z bibliotekami i sterownikami pakietu Microsoft Office (różnych jego wersji) **wykorzystywanymi w oprogramowaniu zintegrowanego systemu finansowo-księgowego (oprogramowanie Simple.ERP), zainstalowanego i wykorzystywanego przez Zamawiającego. Musi zostać praktycznie potwierdzona możliwość prawidłowej, pełnej współpracy obu systemów.**

UWAGI

a) Zamawiający nie dopuszcza dostawy licencji typu OEM.

b) Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.

c) Licencje muszą pozwalać na przenoszenie pomiędzy stacjami roboczymi/serwerami (np. w przypadku wymiany stacji roboczej/serwera).

d) Licencja musi zapewniać możliwość korzystania z wcześniejszych wersji zamawianego oprogramowania.

e) Licencje muszą być przeznaczone do użytku w jednostkach akademickich na terenie Rzeczpospolitej Polskiej

f) **W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie prawidłowo współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca nieodpłatnie przywróci sprawne działanie infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego**.

		Oprogramowanie pakietu biurowego w wersji profesjonalnej, wersja polska, wersja edukacyjna (akademicka) - 34 szt. Licencji wieczystych + nośnik 1 szt.	**TYP oferowany: ……** **Producent: ……..**
		Minimalna charakterystyka wymagana j.w.	**Parametry oferowane nie gorsze, niż wymagane (patrz pkt 1 – 14 powyżej)** Załączone dokumenty (dla rozwiązań równoważnych): …… ……

4.2 Dostawa licencji na oprogramowanie antywirusowe do indywidualnych komputerów i stacji roboczych w wersji edukacyjnej (akademickiej) – w łącznej liczbie 35 szt.

Wstęp.

Zamawiający posiada obecnie i eksploatuje licencje na **oprogramowanie antywirusowe BROADCOM Symantec Endpoint Protection** w wersji 14.3 **(467 szt. licencji akademickich)** z wykupioną pomocą techniczną i aktualizacją do 27.11.2021 r.
W związku z wykonaną instalacją, konfiguracją i pomyślną eksploatacją ww. oprogramowania antywirusowego na przestrzeni kilku lat do chwili obecnej na 467 indywidualnie użytkowanych komputerach (z systemami operacyjnymi MS Windows 7, 8.x, 10 32 lub 64-bit), Zamawiający oczekuje w ramach przedmiotu zamówienia dostawy **rozszerzenia o 35 nowych szt. liczby licencji akademickich (z rocznym abonamentem na pomoc techniczną i aktualizację) do posiadanych przez Instytut 467 szt. Licencji akademickich (EDU) na ww. oprogramowanie antywirusowe** lub dostawy rozwiązania antywirusowego równoważnego w wersji akademickiej, którym będzie można zarządzać w sposób kompatybilny z dotychczas użytkowanym ww. oprogramowaniem.

Opis przedmiotu zamówienia:

Dostawa rozszerzenia liczby licencji akademickich na oprogramowanie antywirusowe posiadane przez Zamawiającego o 35 szt. (z 1 kpl. nośników) z rocznym abonamentem na pomoc techniczną i aktualizację lub dostawa 35 szt. licencji akademickich na oprogramowanie antywirusowe równoważne z rocznym abonamentem na pomoc techniczną i aktualizację.

Przedmiotem zamówienia jest dostawa **bezterminowych** licencji na oprogramowanie **profesjonalnego pakietu antywirusowego (wyprodukowanego przez jednego producenta), o minimalnej funkcjonalności przedstawionej poniżej, w wersji polskiej, aktualnej na rok 2021 tj. najnowszej stabilnej, opublikowanej przez producenta, akademickiej (typu EDU lub ACADEMIC) – przeznaczonej dla jednostek naukowych i edukacyjnych,** w pełni kompatybilnej na poziomie **zarządzania** z wymienionym we Wstępie oprogramowaniem użytkowanym obecnie u Zamawiającego oraz systemem operacyjnym **Microsoft Windows 10** zainstalowanym na dysponowanym obecnie przez Zamawiającego sprzęcie komputerowym.

Wszystkie oferowane Licencje i Oprogramowanie muszą być fabrycznie nowe, nigdy wcześniej nie aktywowane, wszystkie skojarzone z tym samym kluczem aktywacyjnym (lub równoważnym identyfikatorem aktywacyjnym) oraz muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta obejmujących rynek polski, zapewniających w szczególności realizację uprawnień gwarancyjnych.

Przedmiotem zamówienia jest zatem **rozszerzenie o 35 szt. licencji na oprogramowanie pakietu antywirusowego posiadanego przez Zamawiającego** lub dostawa **35 szt.** licencji na **rozwiązanie równoważne** zgodnie z warunkami równoważności przedstawionymi poniżej w Tabeli 2. Licencje na pakiet oferowanego oprogramowania antywirusowego muszą być dostarczone w opcji przysługującej jednostkom akademickim (wersja EDU, ACADEMIC).

Warunki równoważności na oprogramowanie antywirusowe równoważne

Dostawa **rozwiązania antywirusowego równoważnego** obejmuje następujące czynności na zestawie 35 szt. komputerów indywidualnych Zamawiającego z systemami operacyjnymi MS Windows 10, 64-bit:

1. Dostawę 35 szt. Licencji wieczystych na oprogramowanie antywirusowe równoważne o parametrach co najmniej takich, jak wymienione w tabeli nr 2, z 12-miesięcznym abonamentem na wsparcie techniczne i aktualizację baz zagrożeń
2. Wykonanie (przez Wykonawcę) instalacji i skonfigurowania ww. oprogramowania równoważnego na 35 komputerach Zamawiającego w siedzibach Zamawiającego w Warszawie i w Łodzi
3. Przeszkolenie wszystkich użytkowników ww. komputerów oraz dwóch administratorów w zakresie funkcjonalności, własności interfejsu oraz użytkowania ww. oprogramowania antywirusowego równoważnego oraz jego systemu zarządzania
4. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje opóźnienia lub inne zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo - programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego.
5. Wraz z produktem równoważnym Wykonawca jest zobowiązany do dostarczenia następujących dokumentów:
    a. pełnego postanowienia licencji / sublicencji produktu równoważnego,
    b. pełnego wykazu funkcjonalności produktu równoważnego, co najmniej zgodnego z wymaganiami minimalnymi określonymi w Tabeli 2
    c. pełnych warunków i zasad świadczenia usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji dla produktu równoważnego,
    d. wykazu miejsc zastosowania produktu równoważnego.

Tabeli 2. **Minimalna charakterystyka wymagana**

		Oprogramowanie antywirusowe do lokalnego zastosowania na komputerach indywidualnych - najnowsza wersja korporacyjna, wersja polska, wersja edukacyjna (akademicka) - 35 szt. Licencji wieczystych + nośnik 1 szt.	**TYP oferowany: ……. Producent: ……**
	Funkcja / parametr	**Minimalna charakterystyka wymagana**	**Parametry oferowane nie gorsze, niż wymagane** (w polach, w których jest to wymagane, wpisać **wartość**, w pozostałych **wpisać „Tak" lub „Nie")**
	Potwierdzenie skuteczności ochrony	Zamawiający dopuszcza oprogramowanie antywirusowe, którego skuteczność ochrony potwierdzona jest przez renomowane organizacje publiczne zajmujące się bezpieczeństwem komputerowym w niezależnych testach oprogramowania, których aktualne wyniki opublikowano na stronie: • http://www.av-test.org/en/antivirus/business-windows-client/	

	Poziom wykrywalności zagrożeń	Ogólna wykrywalność różnego typu zagrożeń (*Protection*) nie może być mniejsza niż na poziomie ocenionym na 6 pkt, potwierdzona w testach z ostatnich 12 miesięcy (ochrona w czasie rzeczywistym), których wyniki opublikowano na stronie (http://www.av-test.org/en/antivirus/business-windows-client/)	
	Poziom wpływu na spowolnienie pracy systemu komputerowego (pracującego pod systemem Windows 7,8/8.1,10)	Poziom wpływu na spowolnienie pracy systemu komputerowego (*Performance*) nie może być oceniony na mniej niż 6 pkt. wg testów z ostatnich 12 miesięcy, których wyniki opublikowano na stronie (http://www.av-test.org/en/antivirus/business-windows-client/)	
	Funkcjonalność i jakość interfejsu użytkownika	Poziom funkcjonalności i jakości interfejsu użytkownika (*Usability*) nie może być oceniony na mniej niż 6 pkt. wg testów z ostatnich 12 miesięcy, których wyniki opublikowano na stronie (http://www.av-test.org/en/antivirus/business-windows-client/)	
	Wsparcie techniczne i zasady aktualizacji	• min. 1 rok od daty zakupu • kompletne aktualizacje produktu/pakietu w tym okresie • możliwość przedłużenia subskrypcji na kolejny okres wraz z aktualizacją oprogramowania do najnowszej dostępnej wersji	**Oferowany okres wsparcia technicznego i aktualizacji:** **……**
	Zgodność z aktualnym oprogramowaniem Zamawiającego	Zgodność oprogramowania typu Klient z oprogramowaniem Symantec Endpoint Protection Manager z pakietu Symantec Endpoint Protection (wykorzystywanym obecnie w liczbie **467** licencji przez Zamawiającego)	
	Zgodność z systemem operacyjnym	Wymagana pełna zgodność z systemami: Windows 7 32/64-bit, Windows 8/8.1 32/64-bit, Windows 10 32/64-bit, Windows Server 2003 32/64-bit, Windows Server 2008 32/64-bit, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.	
		Wymagane komponenty oprogramowania takie jak: firewall, zapobieganie włamaniom (IPS), kontrola urządzeń i aplikacji oraz kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.	
		Serwer zarządzający musi działać na systemach Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019.	
	Wymagane funkcje/parametry	**Wymagania funkcjonalne dla równoważnego oprogramowania antywirusowego (produktu)**	
	Ochrona antywirusowa:	Usuwanie wirusów, makro-wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samo rozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona przed oprogramowaniem typu "spyware" i "adware", włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu.	

		Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów musi być realizowane w pojedynczym systemie skanującym.	
		Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie.	
		Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane.	
		Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych.	
		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 nośnikach pamięci (np. podłączonych przez port USB).	
		Wymagana możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej.	
		Wymagana możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.	
		Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek.	
		Wymagana funkcjonalność wyszukiwania/usuwania 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.	
		Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie - serwerze czy stacji roboczej.	
		Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące.	
		Wymagana możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących - powrót do poprzedniego zastawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów.	

		Wymagana możliwość natychmiastowego "wypchnięcia" definicji wirusów do stacji klienckich	
		Wymagana aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej trzy razy dziennie.	
		Wymagana możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę.	
		Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.	
		Dedykowany moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanych zagrożeń typu robak internetowy, koń trojański, keylogger - analiza zachowania opiera się na wykonywanych przez aplikację czynnościach (tworzenie nowych plików, komunikacja z internetem, podmiana strony w przeglądarce, itp.).	
		Dedykowany moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą.	
		Automatyczna rejestracja w dzienniku zdarzeń wszelkich nie autoryzowanych prób zmian rejestru dokonywanych przez użytkownika.	
		Automatyczne ponowne uruchomianie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.	
		Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.	
		Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.	
		Skanowanie poczty klienckiej (na komputerze klienckim).	
		Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach.	
		Ściągnięcie dowolnego pliku na komputer musi spowodować sprawdzenie reputacji takiego pliku - jako reputacja rozumie się odpowiedź, co do ilość użytkowników w Internecie korzystających z danej aplikacji/pliku, czasu, kiedy aplikacja/plik pojawiła się w Internecie po raz pierwszy oraz czy aplikacja/plik jest "prawidłowa" czy też nie.	
		Produkt musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikacje, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni.	
		Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.	

		Wymagana możliwość wyboru wielkości definicji antywirusowych, z której będzie korzystał zainstalowany agent - system musi posiadać pełna wersję sygnatur oraz ich wersję uproszczoną znacząco mniejszą o pełnej do instalacji na systemach z niewielką ilością miejsca na dyskach oraz w systemach VDI.	
		Możliwość konfiguracji oraz personalizacji ustawień oprogramowania	
		Małe zapotrzebowanie na zasoby pamięci operacyjnej i systemu	
		System centralnego zarządzania aktualizacjami	
		Ustawienia alternatywnego źródła pobierania baz sygnatur wirusów	
		Automatyczna aktualizacja silnika skanującego oraz bazy sygnatur wirusów	
		Automatyczne skanowanie w tle	
		Automatyczne skanowanie i monitorowanie operacji związanych z uruchamianiem programów, plików oraz operacji zapisu danych na HDD i nośnikach przenośnych	
		Automatyczne, bezobsługowe wykrywanie, analiza i usuwanie makrowirusów	
		Automatyczne leczenie zainfekowanych plików bądź blokada dostępu do pliku	
		Automatyczne przenoszenie zablokowanego pliku do systemu kwarantanny	
		Skanowanie na żądanie: • dysku • plików • folderów	
		Skanowanie: • w czasie rzeczywistym • ruchu internetowego POP3 i http • poczty wychodzącej/przychodzącej • uruchamianych procesów i plików z nimi powiązanych • wszystkich plików na HDD w tym plików systemowych i ukrytych • pamięci operacyjnej, • rekordów rozruchowych dysków • archiwów ZIP, RAR, ARJ, LZH/LHA, MIME/UU, CAB, PKLite, LZEXE • dokumentów pakietu MS Office • danych NTFS	
		Heurystyczne wykrywanie nowych nie sklasyfikowanych wirusów	

		Blokowanie niebezpiecznych skryptów	
		Dzienniki zdarzeń: • zdarzeń • Infekcji • skanera na żądanie	
		Harmonogram zadań • skanowań • aktualizacji	
	System Firewall:	Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.	
		Moduł firewall musi mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.	
		Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać.	
		Program musi pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne.	
		Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli.	
		Konfiguracja zezwalanego i zabronionego ruchu musi się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji.	
		Konfiguracja stacji musi się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji DNS (FQDN) lub domeny DNS.	
		Firewall musi mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach, musi istnieć możliwość dodania własnego komunikatu.	
		W przypadku wykrycia zdefiniowanego ruchu, firewall musi wysłać wiadomość do administratora.	
		Wymagane uniemożliwianie określenia systemu operacyjnego, rodzaju przeglądarki internetowej przez serwery www.	
		Wymagane uniemożliwianie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację.	
		Wymagane uniemożliwianie przejęcia sesji poprzez losowo generowane numery sekwencji TCP	

		Wymagane domyślne reguły zezwalające na ruch DHCP, DNS, WINS.	
	System IPS -ochrona przed włamaniami	Producent musi dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt.	
		Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.	
		Produkt musi mieć możliwość tworzenia własnych wzorców włamań (sygnatur).	
		Sygnatury te mogą działać w trybie blokuj lub rejestruj.	
		Wykrywanie skanowania portów.	
		Ochrona przed atakami typu odmowa usług (Denial of Service).	
		Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC).	
		Wykrywanie trojanów i generowanego przez nie ruchu.	
		Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.	
		Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Musi istnieć możliwość definiowania wyjątków.	
		System ochrony przed włamaniami musi automatycznie integrować się z przeglądarką internetową (przynajmniej z Internet Explorer oraz Firefox) - uniemożliwiając wykonanie w nich (nawet, jeżeli są podatne) szkodliwego dla nich kodu.	
	Ochrona systemu operacyjnego:	Produkt musi umożliwiać uruchamianie i blokowanie wskazanych aplikacji.	
		Produkt musi umożliwiać ładowanie modułów lub bibliotek DLL.	
		Produkt musi umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje.	
		Aplikacje muszą być rozróżniane poprzez nazwę i sygnaturę cyfrową.	
		Produkt musi umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika.	
		Produkt musi kontrolować dostęp do rejestru systemowego.	
		Produkt musi umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne.	
		Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych.	
		Polityki ochrony muszą mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest	

		tworzony wpis w logu.	
		Wymagana możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego.	
		Wymagana możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, by żadna inna aplikacja/biblioteka z poza listy nie mogła uruchomić się na komputerze.	
		Kolekcja aktualnie znajdujących się aplikacji na systemie końcowym musi być możliwa do wywołania bezpośrednio z konsoli zarządzającej - bez konieczności wykonania jakichkolwiek czynności na systemie końcowym.	
		Wymagana możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, by tylko aplikacje znajdujące się na liście nie mogły uruchomić się na komputerze.	
		Wymagana możliwość automatycznego importu list zarówno białej, jaki i czarnej, co zdefiniowany interwał czasu.	
	Integralności komputera:	Oprogramowanie musi umożliwiać wykonywanie szerokiego zakresu testów integralności komputera pod kątem zgodności z polityką bezpieczeństwa urządzeń końcowych, w tym: programów antywirusowych, poprawki firmy Microsoft, dodatki Service Pack firmy Microsoft, osobistych zapór ogniowych.	
		Testy integralności muszą być przeprowadzane cyklicznie, co zdefiniowany okres czasu.	
		Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta.	
		Oprogramowanie musi umożliwiać wykonanie nie standardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać zaawansowaną składnie If ... Then ... Else.	
		W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:	
		○ Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne	
		○ Pliki - istnienie, data, rozmiar, suma kontrolna	
		○ Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego	
		○ Zainstalowane poprawki	
		○ Uruchomiony proces, wersja systemu operacyjnego	
		○ Własna aplikacja	
		W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako dostępne operacje do wykonania, musi istnieć możliwość:	

		○ Uruchamianie dowolnego/własnego skryptu lub programu	
		○ Logowanie zdarzenia	
		○ Ukazanie okienka z wiadomością	
		○ Pobieranie oraz uruchamianie instalacji	
		○ Musi istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.	
		Musi istnieć możliwość wymuszenia instalacji dowolnej aplikacji.	
		W wypadku niezgodności własnego systemu, oprogramowanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.	
		Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.	
		Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć - na ten czas komputer powinien znaleźć się w kwarantannie.	
	Ochrona środowisk wirtualnych:	Produkt musi umożliwiać identyfikacje środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Microsoft Hyper-V, VMWare.	
		Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym.	
		Produkt musi umożliwiać prawidłowe rozliczenia licencji oferowanego systemu dla systemów wirtualnych typu desktop tzw. VOI, w szczególności tzw. "non-persistent".	
		Produkt musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń.	
	Moduł raportujący:	Produkt musi zapewniać graficzne raportowanie.	
		Wbudowane raporty muszą pokazywać co najmniej:	
		○ stan dystrybucji sygnatur antywirusowych, sygnatur heurystycznych oraz IDS/IPS	
		○ wersje zainstalowanych klientów	
		○ inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor)	
		○ wykryte wirusy, zdarzenia sieciowe, integralności komputerów	
		○ zainstalowane technologie i ich aktualny stan	

		Moduł raportowania musi pokazywać stan wykonywanych poleceń na komputerach.	
		Wymagana możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych.	
		Produkt musi umożliwiać automatyczne zbudowanie zapytań, które będą wykonywane o zdanym czasie i ich wynik będzie przechowywany w postacie kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwijanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór intersujących danych). Wszystkie te operacje muszą być wykonywane graficznie.	
		Produkt musi umożliwiać automatyczne budowanie trendów.	
		Produkt musi umożliwiać automatyczne budowanie kluczowych wskaźników wydajności (KPI).	
	Moduł centralnego zarządzania:	Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z konsoli.	
		Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci.	
		Produkt musi wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Musi istnieć możliwość blokowania takich zmian.	
		Produkt musi zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli musi być możliwy po wcześniejszej weryfikacji użytkownika. Produkt musi mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.	
		Wymagana możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym - informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami.	
		Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.	
		Konta administracyjne muszą być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.	
		Uprawnienia administratorów muszą być ustawiane niezależnie dla każdego	
		kontenera wewnątrz organizacji.	
		Wymagana możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.	
		Konfiguracja agentów musi mieć strukturę drzewa, z mechanizmami dziedziczenia.	
		Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika musi być konfigurowany z poziomu centralnej konsoli zarządzającej.	
		Konfiguracja aktywna na stacji musi rozróżniać lokalizację agenta i według tego kryterium	

		określać stosowany zestaw reguł/polityk dla agenta.	
		Lokalizacja musi być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.	
		Opis lokalizacji musi zawierać możliwość tworzenia połączeń logicznych "I" oraz "LUB" na powyżej wymienionych elementach.	
		Paczki instalacyjne produktu muszą pozwalać na dodanie własnej konfiguracji.	
		W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu.	
		Nowe wersje oprogramowania muszą być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.	
		Produkt musi automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.	
		Wymagana możliwość zdefiniowania alertów administracyjnych zawierających co najmniej zdarzenia:	
		• błędnej autoryzacji do systemu zarządzania	
		• dostępności nowego oprogramowania	
		• pojawienia się nowego komputera	
		• zdarzeń powiązanych z infekcjami wirusów	
		• stanu serwerów zarządzających	
		Wymagana możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji.	
		Wymagana oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający.	
		Wymagana **pełna polska wersja językowa** oprogramowania dla **systemu zarządzania i stacji klienckich** wraz z dokumentacją.	