Załącznik nr 1 do zapytania

DOTYCZY: Dostawa sprzętu komputerowego

Opis Przedmiotu Zamówienia

1	TYP:
	KOMPUTER STACJONARNY TYPU ALL-IN-ONE (komputer, w którym podzespoły komputerowe takie jak: płyta główna, procesor czy układ graficzny zostały umieszczone w jednej obudowie z ekranem w taki sposób, który uniemożliwia odłączenie komputera od monitora, posiadający wspólny system zasilania.)
2	Zastosowanie:
	Na potrzeby użytkowania systemu medycznego InfoMedica/AMMS produkcji ASSECO POLAND posiadanego przez Zamawiającego) Korzystanie z usług Active Directory systemu MS Windows Serwer 2019 posiadanego przez Zamawiającego
3	Wydajność obliczeniowa:
	Procesor wielordzeniowy obsługujący zarówno 32-bitowe jak i 64-bitowe aplikacje oraz posiadający sprzętowe wsparcie wirtualizacji. Oferowany procesor musi posiadać minimum 6 rdzeni, minimum 12 wątków, taktowanie minimum 3,0GHz, minimum 18MB pamięci cache. Procesor musi wspierać technologie udostępniania informacji o podzespołach komputera i jego oprogramowaniu, zdalnego dostępu do komputera (monitoring, sterowanie nim, konserwację niezależnie od stanu systemu operacyjnego nawet w gdy komputer jest wyłączony), oraz sprzętowe wsparcie pamięci transakcyjnej. Płyta główna dedykowana do komputera stacjonarnego typu All-In-One, dostosowana do oferowanego procesora, umożliwiająca obsługę magistrali zainstalowanego procesora, wysokowydajnej pamięci zgodnej z oferowanym procesorem, umożliwiająca konfigurację wielodyskową minimum SATA III oraz M.2 PCIe oraz obsługująca minimum 32GB pamięci operacyjnej SO-DIMM. Procesor zaoferowanego komputera musi osiągać w teście wydajności PassMark CPU wynik minimum 20 000 punktów. Wartość punktowa w testach punktowana zgodnie z wykazem do oceny parametrów technicznych
4	Pamięć operacyjna
	Minimum 16 GB pamięci RAM działającej w trybie dual channel w technologii zgodnej z zainstalowanym procesorem z możliwością rozszerzenia do co najmniej 64GB. Ilość wolnych slotów punktowana zgodnie z wykazem do oceny parametrów technicznych
5	Parametry pamięci masowej
	Dysk półprzewodnikowy o pojemności minimum 250GB z interfejsem M.2 PCIe 3.0 x2 NVMe, o prędkościach minimalnych odczyt min 950MB/s, zapis minimum 950MB/s, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego po awarii bez dodatkowych nośników. Prędkości dysku punktowane zgodnie z wykazem do oceny parametrów technicznych
6	Wydajność grafiki
	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią na potrzeby grafiki, umożliwiającą pracę w rozdzielczości minimum 1920x1080 pikseli z maksymalną głębią kolorów 32 bpp przy minimum 60Hz.
7	Karta dźwiękowa / multimedia
	- Karta dźwiękowa zintegrowana z płytą główną, zgodna z HDA - Wbudowane głośniki stereo - Wbudowany minimum jeden mikrofon - Wbudowana kamera 1080p z funkcją zasłonięcia obiektywu, obsługująca Windows Hello
8	Komunikacja
	- Kontroler LAN Ethernet obsługujący standardy 10/100/1000 Mbits z obsługą VLAN 802.1q, zintegrowany z płytą główną

	- Kontroler WIFI 802.11 n/ac podłączony za pomocą zintegrowanego z płytą główną złącza M.2 WLAN, z anteną 2x2 wbudowaną w obudowę komputera, pozwalającą na transmisję z prędkością minimum 1,7 Gbps **Żaden z powyższych kontrolerów nie może być podłączony do komputera poprzez złącze USB (dotyczy złącz zewnętrznych jak i wewnętrznych).** - Kontroler bluetooth 5.x
9	**Porty**
	Zaoferowany komputer musi posiadać minimum: - 1 x DP lub HDMI - 1 x RJ-45 - 4 porty USB (w tym co najmniej 3 porty USB 3.2), w tym przynajmniej jeden umożliwiający szybkie ładowanie urządzeń zewnętrznych/podłączonych nawet przy wyłączonym komputerze - 1 port USB-C Gen.2 **Wymagana ilość (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, hubów itp.** - 1 x Audio (combo)
10	**Peryferia**
	- Klawiatura przewodowa (długość kabla min 1.4 m) USB w układzie polski programisty - Mysz optyczna przewodowa (długość kabla min 1.4 m) USB z rolką (scrool), DPI minimum 1000
11	**Napęd optyczny**
	Wbudowana nagrywarka DVD +/- RW wraz z dołączonym oprogramowaniem (do użytku komercyjnego) do odtwarzania i nagrywania **Nie dopuszcza się wbudowanego napędu wymagającego podłączenia poprzez zewnętrzny port USB.**
12	**Ekran**
	Ekran musi posiadać minimalne parametry: - rozdzielczość FULL HD 1920x1080 - przekątna 21,3 cala (+/- 0,3 cala), format 16:9 - matryca matowa IPS (In Plane Switching) (należy podać typ matrycy: IPS/WVA/PLS/MVA) - 16 mln kolorów - kontrast statyczny 1000:1 - podświetlenie LED
13	**Obudowa**
	Zintegrowana z monitorem typu All-In-One, musi posiadać: - możliwość montażu na ścianie z wykorzystaniem otworów montażowych w standardzie VESA - grubość obudowy nie może przekraczać 60mm (nie wliczając wymiarów stopy) - możliwość bez narzędziowego demontażu stopy, pokrywy komputera - czujnik otwarcia obudowy Podstawa musi umożliwiać: - regulację kąta nachylenia w zakresie minimum od 5st do przodu do minimum 20st do tyłu - regulacje wysokości w zakresie minimum 110mm
14	**BIOS i diagnostyka**

	- BIOS zgodny ze specyfikacją UEFI Możliwość odczytania z Bios informacji o: - modelu komputera, - numerze seryjnym i modelu (PN), - MAC Adres karty sieciowej, - wersja Biosu wraz z datą wydania wersji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - licencji na system operacyjny - stanie wentylatorów (procesora) - napędach lub dyskach podłączonych do portów SATA1-SATA2 - informacji o licencji na system operacyjny Możliwość z poziomu Bios: - wyłączenia selektywnego (pojedynczego) portów USB - wyłączenia selektywnego (pojedynczego) portów SATA - zmiany pracy wentylatorów między trybem optymalizacji głośności lub temperatury - zdefiniowania tygodniowej agendy automatycznego włączania komputera - ustawienia hasła: administratora, Power-On, HDD, - zmiany trybu pracy kontrolera SATA pomiędzy AHCI, Optane - wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanej kamery, - ustawienia portów USB w tryb braku możliwości kopiowania danych na nośniki USB lub całkowitego braku komunikacji z urządzeniami pamięci masowej (na poziomie systemu operacyjnego) - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji startowych (podstawowa, WOL, po awarii) - zablokowania możliwości aktualizacji bios przez użytkownika - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych
15	Zabezpieczenia fizyczne
	Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego np. w postaci blokady zabezpieczającej typu Kensington lub innej. Założona linka zabezpieczająca musi jednocześnie umożliwiać przypięcie komputera AIO np. do biurka oraz zabezpieczenie obudowy przed nieautoryzowanym otwarciem.
16	Zasilanie i eksploatacja
	Urządzenie spełniające wymagania rozporządzenia Komisji (UE) Nr 617/2013 w sprawie wykonania dyrektywy Parlamentu Europejskiego i Rady 2009/125/WE, posiadające oznakowanie CE i wydaną deklarację zgodności WE (załącznik VI do dyrektywy 2009/125/WE)
17	System operacyjny
	Zainstalowany system operacyjny do zastosowań profesjonalnych wg wymagań wyszczególnionych poniżej, z licencją dożywotnią. Licencja zaimplementowana w BIOS płyty głównej komputera, umożliwiająca instalację systemu bez podawania klucza licencyjnego wymaganego oprogramowania (klucz licencyjny automatycznie pobierany z BIOS podczas instalacji). Komputer musi posiadać naklejkę legalności dostarczanego oprogramowania. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostarczanego systemu operacyjnego. Dostarczona licencja musi obejmować wsparcie producenta dla tego systemu operacyjnego do minimum 2026 roku. Wymaga się aby dostarczona wersja systemu była na rynku już od minimum 2 lat. Dostarczona licencja systemu operacyjnego musi umożliwiać instalację i legalne użytkowanie poprzedniej wersji systemu operacyjnego, tzw. downgrade systemu. Preinstalowany fabrycznie na dysku twardym system operacyjny w polskiej wersji językowej. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

	1. Możliwość pracy w systemie Infomedica/AMMS produkcji Asseco Poland (posiadanym przez Zamawiającego) 2. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek 3. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet 4. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) 5. Internetowa aktualizacja zapewniona w języku polskim 6. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe 8. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) 9. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer 10. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta 11. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu 12. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników 13. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych 14. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych 15. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 16. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika 17. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi 18. Wbudowany system pomocy w języku polskim 19. Certyfikat producenta oprogramowania na dostarczany sprzęt 20. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących) 21. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji 22. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny 23. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509 24. Wsparcie dla logowania przy pomocy smartcard 25. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji 26. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk 27. Wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 28. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń 29. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem bez konieczności ponoszenia dodatkowych kosztów 30. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację 31. Graficzne środowisko instalacji i konfiguracji 32. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe 33. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe

	34. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej 35. Możliwość przywracania plików systemowych 36. System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) 37. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu
18	Pakiet biurowy
	Pakiet biurowy wg wymagań wyszczególnionych poniżej z licencją dożywotnią do zastosowań komercyjnych. *Wymagania ogólne:* - Pełne wsparcie dla zaoferowanego systemu operacyjnego. - Pełna polska wersja językowa interfejsu użytkownika. - Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. - 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. - Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim - Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji. - Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. - Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat. - Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta. - Zawierające w pakiecie przynajmniej edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji. - Aplikacja do tworzenia prezentacji powinna umożliwiać udostępnianie prezentacji przy użyciu przeglądarki internetowej bez potrzeby instalowania dodatkowych elementów ani konfigurowania. Do każdej prezentacji można dodać wciągające wideo, aby zwrócić uwagę odbiorców. Nagrania wideo można wstawiać bezpośrednio w programie, a następnie dostosowywać je, przycinać lub oznaczać najważniejsze sceny w nagraniu zakładkami, aby zwrócić na nie szczególną uwagę. Wstawiane nagrania są domyślnie osadzone, dzięki czemu nie trzeba zarządzać dodatkowymi plikami wideo. Pliki programów edytora tekstów, arkusza kalkulacyjnego i programu do tworzenia prezentacji można przechowywać online i uzyskiwać do nich dostęp, przeglądać, edytować i udostępniać innym użytkownikom. *Pakiet biurowy musi spełniać następujące wymagania:* - 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 rozporządzeniem Rady Ministrów 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), • umożliwia wykorzystanie schematów XML, • wspiera w swojej specyfikacji podpis elektroniczny zgodnie z rozporządzeniem Rady Ministrów 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),

- Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.

- W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
- Pakiet zintegrowanych aplikacji biurowych musi zawierać:
  - Edytor tekstów.
  - Arkusz kalkulacyjny.
  - Narzędzie do przygotowywania i prowadzenia prezentacji.
  - Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

- Edytor tekstów musi umożliwiać:
  - Edycję i formatowanie tekstu w języku polskim 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.
  - Formatowanie nagłówków i stopek stron.
  - Sprawdzanie pisowni w języku polskim.
  - Śledzenie zmian wprowadzonych przez użytkowników.
  - 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 Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
  - Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
  - Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
  - Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

- Arkusz kalkulacyjny musi umożliwiać:
  - Tworzenie raportów tabelarycznych.
  - Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.

- 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 tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli 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 Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
- Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

- Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
  - Przygotowywanie prezentacji multimedialnych.
  - Prezentowanie przy użyciu projektora multimedialnego.
  - Drukowanie w formacie umożliwiającym robienie notatek.
  - Zapisanie 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.
  - 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 oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

- Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
  - 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.
  - Automatyczne grupowanie poczty o tym samym tytule.
  - 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 użytkowników. **Zamawiający wymaga fabrycznie nowego oprogramowania biurowego nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu**
19	**Pakiet antywirusowy**
	Zainstalowany pakiet antywirusowy wg wymagań wyszczególnionych poniżej: *Informacja Zamawiającego:* - Zamawiający obecnie posiada pakiet antywirusowy ESET PROTECT do użytku dla biznesu wraz z wdrożoną konsolą do centralnego zarządzania, - Użyte przez Zamawiającego wszelkie nazwy handlowe, znaki towarowe, patenty i miejsce pochodzenia są uzasadnione specyfiką przedmiotu zamówienia i mają na celu wskazanie jedynie jakości przedmiotu zamówienia. *Wymagania ogólne:* W przypadku zaoferowania ESET PROTECT do użytku dla biznesu , Zamawiający wymaga aby: - udzielona licencja obejmowała okres równy okresowi gwarancji, - udzielona licencja umożliwiała użytkowanie programu we wszystkich jednostkach organizacyjnych Zamawiającego, - zaoferowany produkt współpracował z konsolą centralnego zarządzania posiadaną i wdrożoną przez Zamawiającego ESET Security Management Center. W przypadku zaoferowania rozwiązania równoważnego Zamawiający wskazuje wymagania minimalne dla pakietu antywirusowego: **Wymagania ogólne dla stacji roboczych:** - Wsparcie dla 32 i 64-bitowej wersji systemu Windows lub innego dostarczonego razem z komputerami systemu operacyjnego, - Pełne wsparcie dla zaoferowanego systemu operacyjnego - Wersja programu dostępna w całości w języku polskim - Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim - Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA Labs lub Check Mark *Ochrona antywirusowa i antyspyware:* - Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. - Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. - Wbudowana technologia do ochrony przed rootkitami. - Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. - Możliwość skanowania całego dysku, dysków sieciowych oraz nośników zewnętrznych wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. - System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania. - Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami, (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

	- Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. - Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. - Skanowanie plików spakowanych i skompresowanych. - Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń). - Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. - Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. - Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na określony czas lub do ponownego uruchomienia komputera. - W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. - Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. - Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. - Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej. - Automatyczna integracja skanera POP3 i IMAP z klientem pocztowym. - Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie. - Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. - Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. - Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. - Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. - Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. - Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. - Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. - Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. - Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. - Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. - Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. - Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. - W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. - Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie. - Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. - Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. - Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. - Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

	- Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. - Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik komputera przy próbie dostępu do konfiguracji był proszony o podanie hasła. - Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. - Możliwość zabezpieczenia hasłem konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji - Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. - Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. - Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. - System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. - Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych - Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. - Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. - Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. - W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. - Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika - Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). - Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów: - tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, - tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, - tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach. - Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. - Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. - Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. - Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. - Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. - Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. - Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. - Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http - Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). - Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).

	- Program ma wspierać technologię NetWork Access Control. - Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. - W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Ochrona przed spamem: - Ochrona antyspamowa dla różnych programów pocztowych wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych. - Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. - Integracja z różnymi programami pocztowymi - antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. - Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. - Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. - Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. - Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. - Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”. - Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. *Zapora osobista (personal firewall):* - Zapora osobista ma pracować jednym z 5 trybów: - tryb automatyczny - program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, - tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł, - tryb interaktywny - program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), - tryb oparty na regułach - użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, - tryb uczenia się - umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. - Możliwość tworzenia list sieci zaufanych. - Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera. - Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. - Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. - Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. - Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. - Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. - Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. - Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. - Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. - Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. - Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci - Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.

	- Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie. - Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 - Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. - Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera. *Kontrola dostępu do stron internetowych:* - Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. - Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. - Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. - Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. - Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii. - Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. - Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. - Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. *Konsola zdalnej administracji:* Dostępna przynajmniej w jednej z dwóch opcji tj.: a/ w wersji do instalacji/konfiguracji/zarządzania w lokalnym środowisku Zamawiającego - Serwer administracyjny musi oferować możliwość instalacji na różnych platformach systemowych m.in. Windows Server, systemach Linux lub można go pobrać ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). - Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. - Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. b/ w wersji do konfiguracji/zarzadzania w środowisku rozproszonym („w chmurze”) wraz z niezbędna licencją pozwalającą na użytkowanie tej funkcjonalności c/ wymagane funkcjonalności wspólne bez rozróżnienia na środowisko instalacji serwera - Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. - Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. - Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. - Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. - Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. - Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. - Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. - Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. - Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. - Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.

	- Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. - Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. - Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. - Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. - Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. - Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. - Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. - Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. - Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. - Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. - Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej. - Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. - Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. - Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. - Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. - Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. - Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. - Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. - Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej - Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. - Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. - Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. - Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. - Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. - Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. - Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. - Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup. - Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. - Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. - Serwer administracyjny musi informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.

	- Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. - Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. - Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. - Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. - Serwer administracyjny musi oferować możliwość utworzenia różnych grup komputerów. - Grupy tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. - Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. - Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. - Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora. - Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta - Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów. - Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. - Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów. - Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. - Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. - Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. - Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. - Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. - Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. - Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. - Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. - Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. - Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. - Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. - Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. - Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. - Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. - Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).

	- Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. - Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki - Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie. - Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.
20	Wirtualizacja i oprogramowanie
	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
21	Gwarancja
	Min. 36 miesięcy na miejscu u klienta z czasem reakcji do końca następnego dnia roboczego od zgłoszenia. Komputer musi posiadać pakiet serwisowy oferujący następujące warunki gwarancji: - Gwarancja min. 36 miesięcy na części i czynności serwisowe - Czas usunięcia awarii w okresie gwarancji: do 14 dni kalendarzowych, liczony od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt. W przypadku konieczności wysłania komputera do serwisu zewnętrznego Zamawiający zastrzega sobie możliwość wymontowania dysku z komputera na czas jego naprawy - Komputer nie będzie posiadał plomb lub innych elementów ograniczających dostęp do wnętrza - Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta - Możliwość pobierania dokumentacji i sterowników z jednej lokalizacji w sieci Internet Serwis urządzeń musi być realizowany zgodnie z wymaganiami normy ISO 9001
22	Wsparcie techniczne:
	- Możliwość uzyskania pomocy technicznej producenta w języku polskim za pomocą strony WWW, telefonicznie np. infolinii itp. - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera lub autoryzowanego partnera serwisowego producenta - Możliwość weryfikacji czasu obowiązywania gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera lub autoryzowanego partnera serwisowego producenta Należy podać adres strony oraz sposób realizacji wymagania (opis uzyskania w/w informacji)
23	Inne, ergonomia
	- Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie nowszej wersji BIOS. Oprogramowanie to musi łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. - Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca. - Produkt musi być fabrycznie nowy. Niedozwolone jest oferowanie sprzętu z programów Refurbished itp.

	- Kabel zasilający, kabel sieciowy STP kategorii 7 o długości 2 m - Wszystkie oferowane urządzenia muszą być publicznie dostępne. Zamawiający nie dopuszcza stosowania urządzeń dedykowanych, stworzonych na potrzeby niniejszego zamówienia.