Załącznik nr 9 do SIWZ

Wykaz oferowanych produktów
po zmianach w dniu 15 listopada 2017 roku

1. Oprogramowanie

W poniższej tabeli Wykonawca zawarł wykaz oferowanego Oprogramowania Aplikacyjnego jakie oferuje na potrzebę spełnienia wymagań zdefiniowanych w Załączniku nr 1 A-B do SIWZ

Lp.	Producent i nazwa Oprogramowania	Typ Oprogramowania**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

** - Typ oprogramowania wg klasyfikacji zgodnej z IPU : Oprogramowanie Aplikacyjne / Oprogramowanie Dedykowane

2. Infrastruktura sprzętowa

2.1. Serwery – 5 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych wraz z organizerem do mocowania okablowania.	
2	Procesor	Architektura x86, wynik wydajności procesorów zainstalowanych w oferowanym serwerze powinien być nie mniejszy niż 315 punktów Base w testach SPECint_rate2006 opublikowanych przez SPEC.org http://spec.org/cpu2006/results/rint2006.htmldla konfiguracji dwuprocesorowej.	
3	Liczba procesorów	Min. 2	
4	Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje.	
5	Pamięć operacyjna	Zainstalowane 96GB pamięci RAM w układach 16GB Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Obsługa do 1,5TB pamięci operacyjnej potwierdzona w dokumentacji producenta dostępnej na oficjalnej stronie www producenta w dniu składania ofert. Pamięć o częstotliwości min. 2400MHz.	

6	Zabezpieczenie pamięci	ECC, advanced ECC, mirroring, sparing	
7	Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1600x1200 przy 75 Hz i 16 M kolorów.2 porty DB-15 video (z przodu i z tyłu obudowy).	
8	Dyski	W chwili dostawy serwer powinien umożliwiać zainstalowanie do 8 dysków 2.5" Hot Swap bez konieczności instalacji jakichkolwiek dodatkowych komponentów. Zainstalowanych 5 dysków SSD o pojemności min 480GB .	
9	Rozbudowa dysków	Możliwość instalacji dysków SED	
10	Kontroler dyskowy	Zainstalowany sprzętowy kontroler 12 Gb SAS/SATA z możliwością obsługi RAID 0/1/ 5/50 posiadający min 1GB pamięci cache umożliwiający implementacje technologii SSD caching oraz FastPath.	
11	Zasilacz	Dwa zasilacze o mocy min: 550 W (200-240V) typu Platinum oraz dwa przewody zasilające c13-14 o długości min 2.8m	
12	Interfejsy sieciowe	Zintegrowane na płycie 4 porty RJ-45 Gigabit Ethernet 1000BASE-T. Dodatkowy jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Dodatkowo na potrzeby efektywnego zarządzania serwer powinien mieć możliwość współdzielenia jednego portu 10Gb z dodatkowej karty rozszerzeń.	
13	Napędy optyczne	Serwer powinien być wyposażony w napęd dvd z funkcjonalnością nagrywania.	
14	Dodatkowe porty	• z przodu obudowy: 2x USB 2.0 • z tyłu obudowy: 2x USB 3.0, 1x DB-15 video, 1x RJ-45 do karty zarządzającej, 4x RJ-45 GbE porty sieciowe,. Wewnątrz obudowy: 1x USB 2.0 Wymagana możliwość instalacji portu DB-9 serial.	
15	Wewnętrzna pamięć flash	Możliwość instalacji min dwóch karty SD o pojemności minimum 32GB z mechanizmem redundancji.	

16	Chłodzenie	Dostępne 7 wentylatorów. Dwie strefy chłodzenia, dla wentylatorów dostępna redundancja minimum N+1.	
17	Zarządzanie	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0, SNMP i CIM umożliwiający: zdalny restart serwera i zarządzanie serwerem poprzez połączenie w sieci TCP/IP przy użyciu przeglądarki internetowej, jednoczesny dostęp do konsoli przez minimum czterech użytkowników, włączanie/wyłączanie serwera, reinstalację systemu operacyjnego, autentykację użytkowników przy pomocy bezpiecznego połączenia z serwerem LDAP (Lightwieght Directory Access Protocol), monitoring oraz zarządzanie mocą i jej zużyciem. Kontroler zdalnego zarządzania wspierający DNS (Domain Name System) oraz DHCP (Dynamic Host Configuration Protocol) Funkcjonalność przewidywania awarii poprzez monitoring odchyleń od normy działania komponentów takich jak: procesory, pamięć, VRM, dyski, zasilacze i wentylatory. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarządzenie infrastruktura serwerów, przełączników i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 560 urządzeń - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarządzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych - automatyczne wykrywanie dołączanych systemów oraz	

		szczegółową inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń - definiowanie roli użytkowników oprogramowania - obsługa REST API, - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - wsparcie dla NIST 800-131A oraz FIPS 140-2 - obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych -blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub błędem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsługa NTP - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłaniem plików diagnostycznych, - przesyłanie alertów do konsoli firm trzecich	
18	Funkcje zabezpieczeń	Hasło włączania, hasło administratora, dwa moduły TPM(Trusted Platform Modules)	
19	Urządzeniahot	Dyski twarde, zasilacze oraz wentylatory	

	swap		
20	Obsługa	Możliwość wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych	
21	Diagnostyka	Panel diagnostyczny na froncie obudowy w postaci wyświetlacza LED. Serwer musi być wyposażony w system diod LED na płycie głównej wskazujących awarie komponentów takich jak: kości pamięci, procesory, wentylatory, karty SD.	
22	Systemy operacyjne, wirtualizacja	Zainstalowany system operacyjny (SSO) musi posiadać następujące, wbudowane cechy: • Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1 TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. • Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu	

		operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Graficzny interfejs użytkownika. • Zlokalizowane w języku polskim co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe	

		• Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	
23	Waga	maximum: 20 kg	
24	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą serwisu producenta on-site w trybie 24x7x24 z gwarantowanym czasem naprawy w następnym dniu . W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Zarządzanie (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji 7/24 fix 8h oraz zainstalowania dodatkowego dla każdej lokalizacji systemu monitoringu (na dedykowanym serwerze o parametrach rekomendowanych przez producenta oprogramowania monitorującego) W przypadku awarii dyski pozostają własnością Zamawiającego. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
25	Dodatkowe funkcjonalności:	Możliwość instalacji 1 karty GPU	
26	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.1.1. Licencje dostępowe – 350 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

2.2. Macierz dyskowa – 2 sztuki

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obudowa	Macierz musi mieć możliwość zainstalowania w standardowej szafie Rack 19" nie będącej przedmiotem zamówienia. Rozmiar jednostek sterujących macierzą jak i półek rozszerzeń, nie może przekraczać 2U .Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo.	
2	Kontrolery	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz.	
3	Podłączenie hostów	Oferowana macierz musi posiadać w chwili dostawy minimum: a. 4x 1Gbb iSCSI RJ45 b. minimum jeden dedykowany port zarządzający na każdą jednostkę sterująca	
4	Cache	Każdy z modułów sterujących musi być wyposażony w min 8GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania za pomocą technologii nie wymagającej baterii.	
5	Dyski	Macierz musi obsługiwać dyski twarde typu NL-SAS, SAS i SSD oraz	

		umożliwiać instalację różnych typów dysków w ramach jednej półki dyskowej. Macierz musi być wyposażona w minimum 5 dysków 4TB SAS hot-plug Macierz musi umożliwiać obsługę minimum 48 dysków LFF lub 96 dysków SFF.	
6	Funkcjonalność	Macierz musi obsługiwać typy protekcji RAID 0,1,5,6,10. Macierz musi umożliwiać zwiększanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „*thinprovisioning*”). Wymagana możliwość wykonania minimum 128 kopii migawkowych wolumenów z możliwością rozszerzenia tej funkcjonalności do minimum 1024 kopii. Wymagany mechanizm redirect on write. Macierz musi mieć możliwość replikacji asynchronicznej zapisanych na niej danych poprzez sieć IP. Licencja na tę funkcjonalność jest przedmiotem zamówienia. Wymagana możliwość rozszerzenia pojemności cache kontrolerów za pomocą dedykowanych dysków flash macierzy na potrzeby wspomagania wydajności operacji odczytów z systemu dyskowego. Macierz musi posiadać funkcjonalność automatycznego przenoszenia danych na dyski większej wydajności w zależności od częstości dostępu do danych (tzw. „*tiering*”). Wymagane rozwiązanie dokonujące wspomnianego przenoszenia danych w odstępach najwyżej kilku-sekundowych. Opcjonalnie macierz powinna mieć możliwość automatycznego przenoszenia danych na dyski flash. Licencja na tę funkcjonalność nie jest przedmiotem zamówienia. Wymagana możliwość definiowania minimum 16 globalnych dysków hot-spare. Wymagana funkcjonalność szybkiej odbudowy grupy raid poprzez	

		odbudowę tylko obszarów stripe które uległy uszkodzeniu.	
7	Wydajność	Obsługa minimum 1024 logicznych wolumenów o rozmiarze do 140TB Obsługa minimum 32 grup dyskowych Możliwość obsługi minimum 32 grup hostów Możliwość obsługi minimum 256 hostów. Możliwość migracji minimum 32 wolumenów danych w procesie migracji asynchronicznej.	
8	Zarządzanie macierzą	Dostępne dwa porty 1Gbe Base-T – po jednym na kontroler. Zarządzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh GUI powinno umożliwiać ustawienie nazwy systemu, konfiguracje serwera NTP, dodawanie kolejnych zasobów dyskowych, zmianę hasła administratora, tworzenie raid group oraz wolumenów danych, listowanie wolumenów podpiętych do danego hosta. Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp. Wymagana możliwość definiowania poziomu wysyłanych komunikatów np. error, warning, critical error itp. Wymagana możliwość sprawdzenia aktualnego stanu oraz parametrów wydajnościowych macierzy takich jak utylizacja cpu oraz interfejsów połączeniowych, status model oraz parametry każdego dysku macierzy, transfer odczyt/zapis danych do wolumenów w postaci io oraz MBs. Macierz musi posiadać możliwość prezentacji historycznych danych wydajnościowych takich jak ilość operacji wejścia/wyjścia, transfer danych, średni czas dostępu do danych, głębokość kolejki i inne. Wymagana kompatybilność z oprogramowaniem zarządzającym opisanym w wymaganiach odnośnie zarządzania serwerami z	

		załącznika nr 1A.	
9	Inne	Wymagana jest redundancja wszystkich elementów urządzeń tj. kontrolerów, zasilaczy, wentylatorów i ścieżek do dysków. Wymiana tych elementów musi się odbywać bez konieczności wyłączania urządzeń.	
10	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą serwisu producenta on-site w trybie 24x7x24 z gwarantowanym czasem naprawy w następnym dniu . W przypadku awarii, dyski twarde pozostają własnością Zamawiającego. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	

2.3. Zasilacze awaryjne UPS do serwerów – 3 sztuki

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Moc	5000 VA/4500 W wraz z dwoma dodatkowymi modułami baterii	
2	Czas podtrzymania	minimum 19 minut dla obciążenia 4500W	
3	Wysokość	Maksymalnie 8U	
4	Architektura	Podwójna konwersja on-line VFI z wejściem PFC i automatycznym by-passem z możliwością pracy redundantnej ze wspólną baterią	
5	Obudowa	Tower/Rack	
6	Parametry wejściowe	• Napięcie: 230 V (1-fazowe) 181 – 280 V do 100 V przy 50% obciążenia • Częstotliwość : 50 / 60 Hz + /-10% (ustawiana automatycznie) • Współczynnik mocy/THDi : > 0,99 / < 5 %	

		• Zaciski	
7	Parametry wyjściowe:	• Napięcie (czysty przebieg sinusoidalny): 230 V (1-f) do wyboru 200 / 208 / 220 / 240V • Częstotliwość :50 /60 Hz + /- 2 % (+/- 0,05 Hz w trybie pracy bateryjnej) • Współczynnik mocy 0,9 przy 5000 VA • Sprawność: min. 92 % w trybie on-line • Przeciążalność: min. 105 % w sposób ciągły ; 125 % przez 5 min ; 150 % przez 30 s • Gniazda wyjściowe: zaciski	
8	Bateria	• Hermetyczne, bezobsługowe akumulatory o żywotności 5 lat wg klasyfikacji EUROBAT umieszczone w obudowach bateryjnych. Każdy moduł baterii musi składać się z co najmniej 16 szt. akumulatorów 12V/5Ah. • Możliwość dodania 9 szt. dodatkowych modułów baterii, które wydłużą czas podtrzymania do minimum 87 minut dla obciążenia 4500W • Czas ładowania < 6 godz. do odzyskania 90 % wydajności po całkowitym rozładowaniu	
9	Urządzenie musi posiadać alfanumeryczny wyświetlacz LCD wskazujący:	• stan obciążenia, • wyjścia programowalne, • stan baterii, • poziom obciążenia (5 poziomów), • obciążenie obecne, • awaria baterii/wymiana baterii, • alarm ogólny, • przeciążenia, • wartość na wejściu, • tryb normalny/praca z użyciem baterii	

10	Zasilacz UPS musi posiadać diody LED sygnalizujące:	• praca w trybie bypass • brak zakłóceń w zasilaniu, • stan obciążenia	
11	Zasilacz UPS musi posiadać alarmy dźwiękowe sygnalizujące:	• tryb bateryjny, • przeciążenie, • konieczność wymiany baterii	
12	Wyposażenie	Zasilacz UPS musi być wyposażony w wyłącznik alarmu akustycznego, port RS232 (do obsługi protokołu MODBUS), Wraz z zasilaczem UPS musi zostać dostarczona karta komunikacyjna SNMP oraz oprogramowanie do monitorowania i wyłączania stacji roboczych działające w systemach operacyjnych zaproponowanych przez Wykonawcę w ofercie.	
13	Zasilacz UPS musi być zgodny z Normami	• Parametry i topologia: IEC 62040-3 (VFI-SS-111) • Bezpieczeństwo: IEC/EN 62040-1, AS 62040.1.1, AS 62040.1.2 • Kompatybilność elektromagnetyczna IEC/EN 62040-2, AS 62040.2 • Certyfikaty: RoHS, CE, RCM (E2376) • Stopień ochrony IP: min. IP20	
14	Zasilacz UPS musi spełniać parametry środowiskowe co najmniej takie jak :	• Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C) • Wilgotność: 95 % bez kondensacji • Poziom hałasu w odległości 1 m < 55 dB	
15	Wymiary i waga	Wymiary zasilacza UPS (moduł elektroniki) nie może przekraczać sumy wymiarów (cm): 120; 2U Masa zasilacza UPS (moduł elektroniki) – nie większa niż 16 kg Wymiary modułu baterii EBM nie może przekraczać sumy	

		wymiarów (cm): 115; 2U Masa modułu baterii nie może być większa niż 40 kg	
16	Inne	Urządzenie musi mieć możliwość dodania ręcznego bezprzerwowego bypassu serwisowego oraz panelu z gniazdami: IEC 320 C13 - 8 szt., IEC 320 C19 - 2szt. mocowanego na tyle UPS-a. Akcesoria dodatkowe muszą być wyprodukowane przez tego samego producenta co zasilacz UPS.	
17	Gwarancja	Urządzenie musi być objęte gwarancja producenta na okres Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą na moduł elektroniki oraz akumulatory	

2.4. Przełącznik KVM oraz konsola zarządzająca z ekranem LCD- zestaw – 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obudowa	Do instalacji w szafie Rack 19", zestawem montażowym do mocowania w szafie . Wysokość maksymalnie 1U	
2	Ekran, klawiatura	LCD. Wymagana wielkość minimum 18.5 cala. Ekran i klawiatura powinny stanowić zintegrowany moduł umożliwiający konsolidacje w przestrzeni 1U. Na potrzeby zarzadzania konsole powinno się wysuwać przy pomocy odpowiednich szyn mocujących. Wymagana możliwość rozkładania ekranu względem klawiatury pod katem minimum 100 stopni	
3	Rozbudowa	Wymagana możliwość integracji konsoli z przełącznikiem KVM w ramach tej samej przestrzeni Rack 1U.	
4	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obudowa	Do instalacji w szafie Rack 19", zestawem montażowym do	

		mocowania w szafie	
2	Porty	Minimum 8 portów lokalnych. Obsługa łącznie do 128 systemów poprzez połączenie kaskadowe systemów końcowych dla każdego z portów.	
3	Rozbudowa	Wymagana możliwość podłączania minimum 8 przełączników KVM do jednego przełącznika KVM centralnego za pomocą dedykowanych portów.	
4	Zarządzanie	Jeden użytkownik lokalny. Możliwość obsługi użytkowników zdalnych.	
5	Video	Obsługiwane rozdzielczości: 1600x1200 (4:3), 1680x1050 (wide)	
6	Okablowanie	Wymagana obsługa następujących połączeń: KVM Conversion Option, USB Conversion Option, Virtual Media Conversion Option . Obsługa funkcjonalności keep alive dla każdego z typów podłączeń. W momencie dostawy do przełącznika KVM powinno być dołożone 8 sztuk kabli USB Conversion Option.	
7	Bezpieczeństwo	Ochrona hasłem, Obsługa Two Factor Authentication (TFA)	
8	Dodatkowe porty	4x USB, 1x serial port, 1x VGA, 1x Ethernet port,	
9	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	
10	Inne	Ofertowany przełącznik jak i serwery, macierze, napęd taśmowy opisany w załączniku nr 1A, powinny pochodzić od tego samego producenta. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	

2.5. Oprogramowanie do wirtualizacji – 2 sztuki

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.	

2	Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.	
3	Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone dowolną liczbę rdzeni oraz do 2TB pamięci fizycznej RAM.	
4	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych.	
5	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.	
6	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych.	
7	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB.	
8	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.	
9	Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.	
10	Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade).	
11	Polityka licencjonowania oprogramowania nie może wiązać licencji w żaden sposób ze środowiskiem na które zostało zakupione.	
12	Rozwiązanie musi wspierać systemy operacyjne zaproponowane przez Wykonawcę w ofercie.	

13	Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.	
14	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.	
15	Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.	
16	Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.	
17	Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.	
18	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.	
19	Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi (hierarchiczna baza danych).	
20	Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.	
21	System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.	

22	Pojedynczy ww. przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.	
23	Pojedynczy ww. wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.	
24	Ww. wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).	

2.6. Oprogramowanie do backupu – 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.	
2	Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www.	
3	Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania system z poziomu tabletu).	
4	Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych.	
5	Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu).	
6	Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.).	
7	Integracja z usługą katalogową (hierarchiczna baza danych)na poziomie zarządzania dostępem i administratorami.	
8	Wsparcie dla Single Sign On dla logowania do systemu.	

9	Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT.	
10	Definiowanie planów wykonywania kopi zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem).	
11	Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych.	
12	Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym posiadanym przez Zamawiającego.	
13	Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.	
14	Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej).	
15	Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych.	
16	Centralny katalog wszystkich danych zapisanych w kopiach zapasowych.	
17	Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.	
18	Kopie zapasowe całych dysków i partycji.	
19	Kopie zapasowe wybranych plików i folderów.	
20	Kopie zapasowe aplikacji.	
21	Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych.	
22	Zapis kopi zapasowych na udziały sieciowe.	
23	Zapis kopi zapasowych na serwer SFTP.	
24	Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana.	
25	Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery).	
26	Możliwość wyszukiwania plików w kopiach zapasowych.	

27	Szyfrowanie plików kopii zapasowych.	
28	Wsparcie dla technologii VSS.	
29	Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć.	
30	Kompresja plików kopii zapasowych.	
31	Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy).	
32	Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.	
33	Odtworzenie całej maszyny (system zaproponowany przez Wykonawcę w ofercie) – tzw. Bare Metal Restore.	
34	Odtworzenie całej maszyny na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową.	
35	Odtworzenie poszczególnych plików i folderów.	
36	Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania).	
37	Wyszukiwanie i podgląd odtwarzanych wiadomości email.	
38	Ochrona systemów operacyjnych przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń	
39	Możliwość wyboru licencji dożywotnich i subskrypcyjnych	
40	Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji).	

2.7. Napęd taśmowy – 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obudowa	Do zamontowania w szafie Rack (wymagany zestaw montażowy).	
2	Napęd	1x LTO7	
3	Interfejs	2 x SAS 6Gbs 8088	
4	Dodatkowe	Wbudowany port RJ45 na potrzeby zdalnego monitoringu urządzenia. Wsparcie dla nośników LTO WORM (Write Once, Read Many). Wsparcie dla aplikacji AME	
5	Kasety	5 sztuk kaset LTO 7 o parametrach: Retencja danych: 30 lat, Pojemność nagrania: 6 TB, Pojemność po kompresji 2,5: 1: 15 TB, Temperatura/wilgotność pracy: 10-45 C/ 10-80%, oraz 1 sztuka kasety czyszczącej	
6	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą producenta w trybie minimum 9x5 NBD. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	

2.8. Router VPN – 4 sztuki

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Standardy i protokoły	IEEE 802.3, IEEE802.3u, IEEE802.3ab TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP, HTTP, DNS, IPsec, PPTP, L2TP.	
2	Porty	2 gigabitowe porty WAN 2 gigabitowe porty LAN 1 gigabitowy port LAN/DMZ 1 port konsolowy (RJ-45 na RS232)	
3	Okablowanie	10BASE-T: kabel UTP kat. 3, 4, 5 (Maks. 100m)	

	sieciowe	EIA/TIA-568 100Ω STP (Maks. 100m) 100BASE-TX: kabel UTP kat. 5, 5e (Maks. 100m) EIA/TIA-568 100Ω STP (Maks. 100m) 1000BASE-T: kabel UTP kat. 5, 5e, 6 (Maks. 100m)	
4	Przyciski	Reset	
5	Zasilanie	Wbudowany uniwersalny zasilacz AC100-240V~ 50/60Hz na wejściu	
6	Pamięć Flash	8MB	
7	Pamięć DRAM	DDRII 128MB	
8	Diody LED	PWR, SYS, Link/Act, Speed, DMZ	
9	Wymiary (S x G x W)	Suma wymiarów nie może być większa niż 705 mm Standardowa wielkość do szafy - 19 cali szerokości, 1U wysokości	
10	Ilość równoczesnych sesji	60000	
11	Przepustowość NAT	350Mb/s	
12	Przepustowość VPN IPsec (3DES)	130Mb/s	
13	Typ połączenia WAN	Dynamiczne IP, Statyczne IP, PPPoE, PPTP, L2TP, Dual Access, BigPond	
14	DHCP	Serwer/Klientz, DHCP Rezerwacja DHCP	
15	Klonowanie adresów MAC	Możliwość klonowania adresów MAC dla portów WAN/LAN/DMZ	
16	Ustawienia przełącznika	Port Mirror Rate Control Port Config Port VLAN	
17	Równoważenie	Inteligentne równoważenie pasma	

	pasma	Reguły routingu Wiązanie protokołów Przełączanie połączeń WAN - (czasowe, awaryjne) Wykrywanie stanu łącza	
18	NAT	NAT - jeden do jednego NAT - Multinet FTP Serwery wirtualne, Host DMZ, Port Triggering, UPnP /H.323/SIP/IPsec/PPTP ALG	
19	Routing	Routing statyczny Routing dynamiczny (RIP v1/v2)	
20	Tryb pracy system	NAT, Non-NAT, Routing klasyczny	
21	Kontrola ruchu	Kontrola przepustowości w oparciu o IP Możliwość ustalenia ograniczonego i gwarantowanego pasma Harmonogram dostępu Limit sesji w oparciu o IP	
22	IPsec VPN	100 tuneli IPsec VPN LAN-to-LAN, Client-to-LAN 2 tryby negocjacji - Main/Aggressive Szyfrowanie DES, 3DES, AES128, AES192, AES256 Uwierzytelnianie MD5, SHA1 Zarządzanie kluczami - ręczne oraz z wykorzystaniem protokołu IKE IPsec NAT Traversal (NAT-T) Dead Peer Detection (DPD) Perfect Forward Secrecy (PFS)	
23	PPTP VPN	32 tunele PPTP VPN Klient/serwer PPTP VPN PPTP z szyfrowaniem MPPE	
24	L2TP VPN	32 tunele L2TP VPN Klient/serwer L2TP VPN L2TP over IPse	

25	VPN Pass-through	IPsec (ESP), PPTP, L2TP	
26	Port DMZ	1 sprzętowy port DMZ	
27	Kontrola aplikacji	Blokowanie - IM, P2P, Web IM, Web SNS, Web Media, Protocol, Proxy	
28	Ochrona przed atakami sieciowymi	Ochrona przed atakami TCP/UDP/ICMP Flood Blokowanie skanowania TCP (Stealth FIN/Xmas/Null) Blokowanie pakietów ping po stronie WAN	
29	Filtrowanie	Filtrowanie adresów MAC Filtrowanie adresów URL/słów kluczowych Filtrowanie zawartości stron (Java, ActiveX, Cookies)	
30	Ochrona przed atakami ARP	Wysyłanie pakietów GARP Skanowanie ARP po stronie LAN/WAN Wiązanie adresów IP-MAC	
31	Usługi	Serwer PPPoE E-Bulletin Dynamiczny DNS (Dyndns, No-IP, Peanuthull, Comexe)	
32	Wsparcie	Zarządzanie przez interfejsy Web/CLI/Telnet Zarządzanie zdalne Eksport/import konfiguracji Synchronizacja NTP Dziennik systemowy	
33	Certyfikaty	CE, FCC, RoHS	
34	Zawartość dostawy	Urządzenie Płyta CD Zasilacz Kabel uziemienia Zestaw elementów montażowych Instrukcja	
35	Wymagania systemowe	Kompatybilny z systemami operacyjnym zaproponowanymi przez Wykonawcę w ofercie.	
36	Środowisko pracy	Dopuszczalna temperatura pracy: 0°C~40°C (32°F~104°F)	

		Dopuszczalna temperatura przechowywania: -40℃~70℃ (-40°F~158°F) Dopuszczalna wilgotność powietrza: 10%~90%, niekondensująca Dopuszczalna wilgotność przechowywania: 5%~90%, niekondensująca	
37	Inne	- Możliwość utworzenia do 100 tuneli IPsec VPN jednocześnie, przepustowość IPsec VPN do 130Mb/s, - IPsec, PPTP, L2TP, L2TP over IPsec, - IPsec NAT Traversal (NAT-T), - Szyfrowanie DES, 3DES, AES128, AES192, AES256, - Uwierzytelnianie MD5, SHA1, - Zarządzanie kluczami - ręczne oraz z wykorzystaniem protokołu IKE, - IPsec VPN - LAN-to-LAN, Client-to-LAN, - Serwer/Klient VPN - PPTP/L2TP, - Sprzętowy port DMZ, - NAT - jeden-do jednego, - FTP/H.323/SIP/IPsec/PPTP ALG, - Blokowanie aplikacji - IM/P2P, - Filtrowanie adresów URL/słów kluczowych, - Filtrowanie zawartości stron internetowych (Java, ActiveX, Cookies), - ARP Inspection, - Ochrona przed atakami DoS/DDoS, - Inteligentna kontrola pasma, - Reguły routing,	

		- Przełączanie połączeń WAN - (czasowe, awaryjne), - Kontrola pasma w oparciu o IP, - Możliwość ustalenia ograniczonego i gwarantowanego pasma, - Limit sesji w oparciu o IP, - Port VLAN, mirroring portów, - Routing statyczny, obsługa RIP v1/v2, - Serwer PPPoE - E-Bulletin	
38	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.9. Zestawy komputerowe – 160 sztuk

2.9.1. Jednostka centralna- 150 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

Lp.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.	
2.	Obudowa	Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu. Wyposażona w min. 2 kieszenie: 1 szt. 5,25” zewnętrzna (dopuszcza się w wersji tzw. slim zajętej przez napęd optyczny), 1 szt. 3,5”, możliwość rozbudowy komputera do konfiguracji dwudyskowej w oparciu o dyski w	

		rozmiarach 2.5” + 3,5”. Obudowa musi być wyposażona w czujnik otwarcia obudowy. Obudowa musi mieć możliwość zainstalowania oryginalnego filtra przeciwpyłowego zapobiegającego nadmiernemu gromadzeniu się kurzu w środku obudowy. Filtr musi umożliwiać łatwe czyszczenie bez otwierania obudowy. Wymagana możliwość czyszczenia filtra za pomocą wody. Filtr musi być także opcją producenta komputera możliwą do zamówienia jako część eksploatacyjna. W ofercie należy podać numer katalogowy (PN) części pod jaką można zamówić filtr u producenta komputera. Beznarzędziowe otwieranie obudowy oraz wymiana HDD, ODD i kart rozszerzających. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem katalogowym PN, numerem seryjnym. Obudowa gotowa do pracy w trybie Pion lub Poziom.	
3.	Chipset	Dostosowany do zaoferowanego procesora	
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Wyposażona złącza dla kart PCIe oraz umożliwiająca ich montaż obudowa: 1 x PCI Express 3.0 x16,2 x PCI Express 2.0 x1,	
5.	Procesor	Procesor osiągający w teście PassMark CPU Mark wynik min. 5900 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: www.cpubenchmark.net).	
6.	Pamięć operacyjna	Min. 4 GB RAM, 2400MHz DDR4, 4 sloty na pamięć, z czego 3wolne. Możliwość rozbudowy do 64 GB.	
7.	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
8.	Napęd optyczny	Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie.	

9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 1220 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/)	
10.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
11.	Karta sieciowa	10/100/1000 – złącze RJ45	
12.	Porty/złącza	Wbudowane porty: 1 x VGA, 2 x DP, 8 x USB w tym: - z przodu obudowy min.:4x USB3.1 Gen 1 - z tyłu obudowy min.:2x USB3.1 Gen 1, 2x USB2.0 - 1 x port sieciowy RJ-45, - 2 x port szeregowy RS-232 - 1 x port równoległy - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
13.	Klawiatura/mysz	Klawiatura przewodowa USB w układzie US, wyposażona w czytnik kart mikroprocesorowych; mysz przewodowa USB z rolką (scroll)	
14.	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 210W oraz sprawności na poziomie: • 20% obciążenia 83% sprawności, • na poziomie 50% obciążenia 85% sprawności • na poziomie 100% obciążenia 83% sprawności. Zasilacz musi posiadać certyfikat 80 PLUS klasy min BRONZE. Należy dołączyć certyfikat ze strony https://plugloadsolutions.com/80pluspowersupplies.aspxpotwierdzający spełnianie w/w wymogu.	
15.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i	

		myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania	

		nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.	

		26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o:	

		a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
16.	Oprogramowanie antywirusowe	1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 36 MIESIĘCY 2. Wsparcie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10. 3. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim. **Ochrona antywirusowa i antyspyware** 4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 5. Wbudowana technologia do ochrony przed rootkitami. 6. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i	

		wykonywanych plików. 8. 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. 9. 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 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 15. 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. 16. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 17. Automatyczna integracja skanera POP3 i IMAP z dowolnym	

		klientem pocztowym bez konieczności zmian w konfiguracji. 18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 20. 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. 21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu	

		kontekstowego. 28. 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. 29. 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. 30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 33. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. 34. 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. 35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 36. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu. 37. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 40. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 41. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika	

		42. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 43. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 44. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 45. 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. 46. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 47. 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. 48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 51. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 52. Program musi być wyposażona w funkcjonalność umożliwiającą	

		tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back). 53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 54. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 55. 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. 56. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 57. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 58. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 59. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 60. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą	

		hasła do ustawień zaawansowanych. **Ochrona przed spamem** 61. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 62. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 63. 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. 64. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 65. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 66. 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”. 67. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. **Zapora osobista (personal firewall)** 68. Zapora osobista ma pracować jednym z 4 trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia	

		utworzenie dodatkowych reguł przez administratora • 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. 69. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący 70. Możliwość tworzenia list sieci zaufanych. 71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 72. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 73. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 78. Możliwość tworzenia profili pracy zapory osobistej w zależności	

		od wykrytej sieci. 79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 80. 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, konkretny interfejs sieciowy w systemie. 81. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. 82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. **Kontrola dostępu do stron internetowych** 83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. 84. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 86. 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. 87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. 88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 89. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny. **Ochrona serwera plików** 1. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie. 2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami i exploitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Program musi posiadać funkcjonalność pozwalającą na	

		ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 13. Aplikacja powinna wspierać mechanizm klastrowania. 14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 18. 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. 19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 23. Automatyczne wyłączenia mają być aktywne od momentu	

		wykrycia usług serwerowych. 24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 27. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 28. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 29. 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. 30. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 31. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 32. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.	

		33. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 34. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 35. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. 36. Po instalacji systemu antywirusowego, 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. 37. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 38. System antywirusowy 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. 39. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 40. System antywirusowy 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. 41. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program	

		antywirusowy z wbudowanym serwerem HTTP). 42. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 43. Aplikacja musi wspierać skanowanie magazynu Hyper-V 44. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 45. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 46. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 47. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna** 1. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 3. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 5. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 6. Podczas logowania administrator musi mieć możliwość wyboru	

		języka w jakim zostanie wyświetlony panel zarządzający. 7. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 8. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 9. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 10. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci – serwer pośredniczący (proxy) lub serwer centralny. 11. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 12. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 13. 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. 14. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 15. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 16. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 17. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 18. Agent musi posiadać możliwość pobrania listy zainstalowanego	

		oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 19. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 20. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 21. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 22. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 23. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 24. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 25. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej. 26. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 27. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 28. Administrator musi posiadać możliwość przypisania kilku	

		zestawów uprawnień do jednego użytkownika. 29. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 30. 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. 31. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 32. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 33. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 34. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 35. Grupy dynamiczne 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. 36. 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. 37. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 38. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta.	

		Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 39. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 40. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 41. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 42. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 43. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 44. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 45. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 46. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 47. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 48. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.	

		49. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 50. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 51. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie). 52. 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. 53. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM Radar	
17.	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: modelu komputera, PN, numerze seryjnym, Asset Tag, MAC Adres karty sieciowej, wersja Biosu wraz z datą produkcji, zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, ilości pamięci RAM wraz z taktowaniem, stanie pracy wentylatora na procesorze, stanie pracy wentylatorów w obudowie komputera, napędach lub dyskach podłączonych do portów M.2 oraz SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy; wyłączenia kontrolera selektywnego (pojedynczego) portów SATA; konfiguracji kontrolera SATA; wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanego głośnika, PXE; możliwość ustawienia portów USB w jednym z dwóch trybów:	

		1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej ustawienia hasła: administratora, Power-On, HDD; blokady aktualizacji BIOS bez podania hasła administratora; 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 botujących (podstawowa, WOL, po awarii); 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.	
18.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów	

		któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	
19.	Certyfikaty i standardy	– Certyfikat ISO9001:2000 dla producenta sprzętu – ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora z umiejscowieniem komputera na biurku w trybie IDLE 23 dB - dołączyć certyfikat lub dokument potwierdzający głośność jednostki - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	-
20.	Waga/rozmiary urządzenia	Waga urządzenia max. 7kg Suma wymiarów nie może przekraczać: 735mm	
21.	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock umożliwiające zastosowanie zabezpieczenia fizycznego w postaci linki metalowej uniemożliwiającej również otwarcie obudowy - Dedykowane oczko na kłódkę umożliwiającą zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy - Moduł TPM 2.0	

22.	Oprogramowanie	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.	
23.	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym.Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
24.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
25.	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.9.2. Monitor – 150 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Przekątna ekranu i wymiary aktywnego obszaru wyświetlania	21,5“ 476 mm x 268 mm	
2	zalecana rozdzielczość	1920 x 1080 (Full HD)	
3	Typowy pobór mocy / w trybie Power management	19 W / 0,5 W	
4	złącza	VGA, HDMI	
5	kontrast typowy	600 : 1	
6	kontrast ACR	10 000 000 : 1	
7	Jasność typowa	200 cd/m2	
8	wielkość plamki	0,248 mm	
9	Czas reakcji	5 ms	
10	Kąt widzenia przy CR>10	poziomo/pionowo: min. 90°/65°	
11	Regulacja cyfrowa OSD	TAK	
12	Certyfikaty i standardy	- CE, - EnergyStar 6.0 - TCO - EPEAT Silver	
13	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.9.3. Jednostka centralna- 10 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

Lp.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.	
2	Obudowa	Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu. Wyposażona w min. 2 kieszenie: 1 szt. 5,25” zewnętrzna (dopuszcza się w wersji tzw. slim zajętej przez napęd optyczny), 1 szt. 3,5”, możliwość rozbudowy komputera do konfiguracji dwudyskowej w oparciu o dyski w rozmiarach 2.5” + 3,5”. Obudowa musi być wyposażona w czujnik otwarcia obudowy. Obudowa musi mieć możliwość zainstalowania oryginalnego filtra przeciwpyłowego zapobiegającego nadmiernemu gromadzeniu się kurzu w środku obudowy. Filtr musi umożliwiać łatwe czyszczenie bez otwierania obudowy. Wymagana możliwość czyszczenia filtra za pomocą wody. Filtr musi być także opcją producenta komputera możliwą do zamówienia jako część eksploatacyjna. W ofercie należy podać numer katalogowy (PN) części pod jaką można zamówić filtr u producenta komputera. Beznarzędziowe otwieranie obudowy oraz wymiana HDD, ODD i kart rozszerzających. Obudowa trwale oznaczona nazwą producenta, nazwą komputera,	

		numerem katalogowym PN, numerem seryjnym. Obudowa gotowa do pracy w trybie Pion lub Poziom.	
3	Chipset	Dostosowany do zaoferowanego procesora.	
4	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Wyposażona złącza dla kart PCIe oraz umożliwiająca ich montaż obudowa: 1x PCI Express 3.0 x16, 2 x PCI Express 2.0 x1,	
5	Procesor	Procesor osiągający w teście PassMark CPU Mark wynik min. 5900 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: www.cpubenchmark.net).	
6	Pamięć operacyjna	Min. 4 GB RAM, 2400MHz DDR4, 4 sloty na pamięć, z czego 3wolne. Możliwość rozbudowy do 64 GB.	
7	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
8	Napęd optyczny	Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie.	
9	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 1220 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/)	
10	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
11	Karta sieciowa	10/100/1000 – złącze RJ45	
12	Porty/złącza	Wbudowane porty: 1 x VGA, 2 x DP, 8 x USB w tym: - z przodu obudowy min.: 4x USB3.1 Gen 1 - z tyłu obudowy min.: 2x USB3.1 Gen 1, 2x USB2.0 - 1 x port sieciowy RJ-45, - 2 x port szeregowy RS-232	

		- 1 x port równoległy - porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
13	Klawiatura/mysz	Klawiatura przewodowa USB w układzie US, wyposażona w czytnik kart mikroprocesorowych; mysz przewodowa USB z rolką (scroll)	
14	Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 210W oraz sprawności na poziomie: • 20% obciążenia 83% sprawności, • na poziomie 50% obciążenia 85% sprawności • na poziomie 100% obciążenia 83% sprawności. Zasilacz musi posiadać certyfikat 80 PLUS klasy min BRONZE. Należy dołączyć certyfikat ze strony https://plugloadsolutions.com/80pluspowersupplies.aspxpotwierdzający spełnianie w/w wymogu.	
15	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami	

		za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów	

		roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z	

		predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne	

		39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
16	Oprogramowanie antywirusowe	1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 36 MIESIĘCY 2. Wsparcie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10 3. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim. **Ochrona antywirusowa i antyspyware** 4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 5. Wbudowana technologia do ochrony przed rootkitami. 6. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. 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.	

		9. 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 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 15. 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. 16. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	

		18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 20. 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. 21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.	

		27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 28. 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. 29. 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. 30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 33. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i	

		administratora wraz z listą niezainstalowanych aktualizacji. 34. 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. 35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 36. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu. 37. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 40. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i	

		umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 41. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 42. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 43. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 44. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 45. 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. 46. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 47. 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. 48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji	

		program zgłosi posiadanie nieaktualnej bazy sygnatur. 50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 51. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 52. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back). 53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 54. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 55. 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. 56. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 57. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 58. W programie musi istnieć możliwość tymczasowego	

		wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. 59. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 60. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. **Ochrona przed spamem** 61. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 62. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 63. 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. 64. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 65. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 66. 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”. 67. Program musi posiadać funkcjonalność wyłączenia modułu	

		antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. **Zapora osobista (personal firewall)** 68. Zapora osobista ma pracować jednym z 4 trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • 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. 69. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący 70. Możliwość tworzenia list sieci zaufanych. 71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 72. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 73. Możliwość zdefiniowania wielu niezależnych zestawów	

		reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 78. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 80. 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, konkretny interfejs sieciowy w systemie. 81. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. 82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. **Kontrola dostępu do stron internetowych** 83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. 84. Moduł kontroli dostępu do stron internetowych musi	

		posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 86. 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. 87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. 88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 89. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny. **Ochrona serwera plików** 48. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie. 49. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 50. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	

		51. Wbudowana technologia do ochrony przed rootkitami i exploitami. 52. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 53. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 54. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 55. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 56. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 57. Możliwość skanowania dysków sieciowych i dysków przenośnych. 58. Skanowanie plików spakowanych i skompresowanych. 59. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 60. Aplikacja powinna wspierać mechanizm klastrowania. 61. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 62. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 63. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	

		64. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 65. 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. 66. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 67. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 68. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 69. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 70. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 71. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 72. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 73. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 74. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 75. Możliwość przeniesienia zainfekowanych plików w	

		bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 76. 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. 77. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 78. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 79. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 80. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 81. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 82. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym	

		użytkownika wraz z listą niezainstalowanych aktualizacji. 83. Po instalacji systemu antywirusowego, 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. 84. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 85. System antywirusowy 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. 86. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 87. System antywirusowy 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. 88. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 89. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 90. Aplikacja musi wspierać skanowanie magazynu Hyper-V 91. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów	

		92. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 93. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 94. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna** 54. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie. 55. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 56. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 57. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 58. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 59. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel	

		zarządzający. 60. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 61. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 62. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 63. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 64. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 65. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 66. 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. 67. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 68. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 69. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 70. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem	

		dedykowanego agenta. 71. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 72. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 73. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 74. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 75. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 76. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 77. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 78. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej.	

		79. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 80. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 81. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 82. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 83. 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. 84. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 85. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 86. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 87. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 88. Grupy dynamiczne 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.	

		89. 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. 90. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 91. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 92. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 93. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 94. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 95. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 96. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 97. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.	

		98. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 99. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 100. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 101. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 102. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 103. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 104. 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.	
17	Oprogramowanie biurowe	Pakiet biurowy musi zawierać co najmniej: a) Edytortekstów, b) Arkuszkalkulacyjny, c) Narzędzie do przygotowania i prowadzeniaprezentacji, d) Narządziedozarządzaniapocztąelektroniczną,kalendarzami izadaniami	

		Ogólne: a) Interfejs w językupolskim, b) wbudowana pomockontekstowa, c) możliwość instalacji na dostarczonym sprzęcie i systemieoperacyjnym Edytor tekstów: a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego), c) tworzenie szablonówdokumentów, d) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, e) wbudowana biblioteka obiektów graficznych isymboli, f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach, g) edycja nagłówków I stopek, h) automatyczne numerowanie rozdziałów, tabel irysunków, i) automatycznetworzeniespisutreści,przypisówiodnośników dotekstu, j) śledzenie wprowadzonychzmian, k) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji), l) tworzenie korespondencjiseryjnej, m) tworzeniemakr, n) podgląd graficzny oraz wydrukdokumentów Arkusz kalkulacyjny:	

		a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami), b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe orazczasowe, c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych iczasowych, d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje natabelach, e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D), f) formatowanie warunkowe komórekarkusza, g) śledzenie formuł oraz automatyczna weryfikacja ichpoprawności, h) tworzenie tabelprzestawnych, i) raporty z wykorzystaniem wyszukiwaniawarunkowego, j) automatyczne filtrowaniadanych, k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, bazdanych, l) zapis wielu arkuszy w jednympliku, m) tworzenie szablonówdokumentów, n) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, o) tworzenie oraz edycji nagłówków istopek, p) osadzanie:symboli,tabel,rysunków,obiektówgraficznychorazwzorówmatematycznych, q) zabezpieczenie plików hasłem (zarówno do odczytu jak	

		iedycji), r) tworzenie korespondencjiseryjnej, s) tworzeniemakr, t) podgląd graficzny oraz wydrukdokumentów, Narzędzie do przygotowania i prowadzenia prezentacji: a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego), c) tworzenie szablonówprezentacji, d) tworzenie animacji dla pojedynczych elementów jak i całychslajdów, e) wbudowana biblioteka obiektów graficznych isymboli, f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych orazfilmów), g) formatowanie tekstów, obiektów graficznych oraztabel, h) umieszczanie notatek oraz podkładudźwiękowego, i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracjidwumonitorowej), j) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach, l) tworzenie oraz edycji nagłówków istopek, m) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji), n) podgląd graficzny oraz wydruk dokumentów (z możliwością	

		wydruku kilku slajdów na jednej stronie oraznotatkami), Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami: a) pełna obsługa plików w formacie.pst, b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP, c) automatyczne filtrowaniepoczty, d) edycja i formatowanie tekstuwiadomości, e) tworzenie i obsługakatalogów, f) tworzenie szablonówdokumentów, g) tworzenie automatycznych reguł zarządzającychpocztą, h) oznaczanie wybranej poczty zdefiniowanymiatrybutami, i) importiobsługawielukalendarzy(wtymkalendarzyzdalnychwformacieiCal), j) udostępnianie kalendarza innymużytkownikom, k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawienia przypomnień), l) automatyczne wysyłanie i odbieranie informacji ospotkaniach, m) tworzenie i zarządzaniezadaniami, n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrup odbiorców), o) odbiór i wysyłanie elektronicznych wizytówek w formacievCard, p) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, q) podgląd graficzny oraz wydruk dokumentów Inne Licencja dożywotnia na pakiet biurowy	

		Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe	
18	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: modelu komputera, PN, numerze seryjnym, Asset Tag, MAC Adres karty sieciowej, wersja Biosu wraz z datą produkcji, zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, ilości pamięci RAM wraz z taktowaniem, stanie pracy wentylatora na procesorze, stanie pracy wentylatorów w obudowie komputera, napędach lub dyskach podłączonych do portów M.2 oraz SATA (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy; wyłączenia kontrolera selektywnego (pojedynczego) portów SATA; konfiguracji kontrolera SATA; wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanego głośnika, PXE; możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej ustawienia hasła: administratora, Power-On, HDD; blokady aktualizacji BIOS bez podania hasła administratora; 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 botujących (podstawowa, WOL, po awarii); 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.	
19	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie • Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware,	

		pojemność, temperatura pracy • Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	
20	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu – ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora z umiejscowieniem komputera na biurku w trybie IDLE 23 dB - dołączyć certyfikat lub dokument potwierdzający głośność jednostki - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	-
21	Waga/rozmiary urządzenia	Waga urządzenia max. 7kg Suma wymiarów nie może przekraczać: 735mm	
22	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock umożliwiające zastosowanie zabezpieczenia fizycznego w postaci linki metalowej uniemożliwiającej również otwarcie obudowy - Dedykowane oczko na kłódkę umożliwiającą zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy - Moduł TPM 2.0	-
23	Oprogramowanie	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.	
24	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
25	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
26	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.9.4. Monitor – 10 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru

1	Przekątna ekranu i wymiary aktywnego obszaru wyświetlania	21,5“ 476 mm x 268 mm	
2	zalecana rozdzielczość	1920 x 1080 (Full HD)	
3	Typowy pobór mocy / w trybie Power management	19 W / 0,5 W	
4	złącza	VGA, HDMI	
5	kontrast typowy	600 : 1	
6	kontrast ACR	10 000 000 : 1	
7	Jasność typowa	200 cd/m2	
8	wielkość plamki	0,248 mm	
9	Czas reakcji	5 ms	
10	Kąt widzenia przy CR>10	poziomo/pionowo: min. 90°/65°	
11	Regulacja cyfrowa OSD	TAK	
12	Certyfikaty i standardy	- CE, - EnergyStar 6.0 - TCO - EPEAT Silver	
13	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.10. Zestawy – stanowiska komputerowe laptopy – 10 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

Lp.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego notebooka.	
2	Ekran	Matryca TFT 15,6" z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: - HD 1366x768, 220nits, kontrast 350:1 Kąt otwarcia matrycy min.180 stopni.	
3	Obudowa	Komputer wykonany z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged", według normy Mil-Std-810G tj. taki, który zaliczył (co najmniej) następujące testy z wynikiem pozytywnym: · Uderzenia- Metoda 516.6 · Zmienna Temperatura- Metoda 503.5 · Wilgotność- Metoda 507.5 W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez zamawiającego. Oświadczenie Wykonawcy potwierdzone oświadczeniem lub innym dokumentem pochodzącym od producenta, potwierdzające, że komputer spełnia standardy MIL-STD-810G, i pozytywnie przeszedł testy w zakresie minimum wyżej wymienionych. Komputer wyposażony w czujnik otwarcia obudowy	

		zabezpieczający przed nieautoryzowanym dostępem. Praca czujnika konfigurowana z poziomu BIOS.	
4	Chipset	Dostosowany do zaoferowanego procesora	
5	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejsy SATA III (6 Gb/s), M.2 do obsługi dysków SATA lub WWAN.	
6	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,4 GHz, pamięcią cache L3 co najmniej 3 MB lub równoważny wydajnościowo osiągający wynik co najmniej 3800 pkt w teście SysMark w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net	
7	Pamięć operacyjna	Min 4GB z możliwością rozbudowy do 32GB, rodzaj pamięci DDR4, 2133MHz. Komputer wyposażony w minimum dwa banki pamięci umożliwiające pracę w trybie dual-channel.	
8	Dysk twardy	Min 256GB SSD M.2 NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
9	Napęd optyczny	Wbudowana nagrywarka DVD	
10	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Karta graficzną osiągająca min. 930 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/)	
11	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1.5W, wbudowane dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p pracująca przy niskim oświetleniu.	
12	Karta sieciowa	10/100/1000 – RJ 45	
13	Porty/złącza	4xUSB 3.1 Gen 1 (jeden z możliwością ładowania urządzeń	

		zewnętrznych poprzez port USB przy wyłączonym komputerze), złącze słuchawek i mikrofonu (combo), VGA, Mini Display Port, RJ-45, czytnik kart multimedialnych (min. SD/SDHC/SDXC/MMC), czytnik kart chipowych, dedykowane złącze dokowania umieszczone w spodniej części notebooka (nie dopuszcza się replikatora portów podłączanego poprzez port USB), Smart card reader. Złącze umożliwiające podpięcie linki antykradzieżowej.	
14	Dokowanie	Dedykowane złącze stacji dokującej dostępne od spodu notebooka, wyposażone w systemem chroniącym styki przed zanieczyszczeniem.	
15	Klawiatura	Klawiatura odporna na zalanie, układ US, z wbudowanym trackpointem, touchpad z obsługą gestów. Klawiatura posiada wydzieloną część numeryczną.	
16	WiFi	Wbudowana karta sieciowa, pracująca w standardzie AC 2x2	
17	Bluetooth	Wbudowany moduł Bluetooth 4.1	
18	Modem LTE	Możliwość rozbudowy notebooka o zintegrowany z obudową komputera modem LTE wraz ze slotem na kartę typu SIM (nie dopuszcza się modemów wykorzystujących Express Card oraz USB port)	
19	Bateria	Notebook wyposażony baterie o pojemności min. 48 Wh - pozwalające na nieprzerwaną pracę urządzenia do 14 godziny – załączyć test Mobile Mark 2014 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym.	
20	Zasilacz	Zasilacz zewnętrzny maks. 45W	
21	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:	

		a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.	

		12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do	

		stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.	

		34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
22	Oprogramowanie antywirusowe	1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 36 MIESIĘCY 2. Wsparcie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10 3. Wersja programu dla stacji roboczych dostępna	

		zarówno w języku polskim jak i angielskim. **Ochrona antywirusowa i antyspyware** 4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 5. Wbudowana technologia do ochrony przed rootkitami. 6. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. 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. 9. 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 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.	

		14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 15. 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. 16. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 20. 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. 21. Automatyczna integracja z dowolną przeglądarką	

		internetową bez konieczności zmian w konfiguracji. 22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 28. 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. 29. 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. 30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 33. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. 34. 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. 35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 36. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu. 37. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 40. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 41. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 42. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 43. Oprogramowanie musi posiadać zaawansowany skaner	

		pamięci. 44. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 45. 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. 46. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 47. 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. 48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 51. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http	

		52. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back). 53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 54. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 55. 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. 56. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 57. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 58. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.	

		59. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 60. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. **Ochrona przed spamem** 61. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 62. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 63. 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. 64. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. 65. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. 66. 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”.	

		67. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. **Zapora osobista (personal firewall)** 68. Zapora osobista ma pracować jednym z 4 trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • 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. 69. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący 70. Możliwość tworzenia list sieci zaufanych. 71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie 72. Możliwość określenia w regułach zapory osobistej	

		kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 73. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. 74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 78. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 80. 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, konkretny interfejs sieciowy w systemie. 81. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. 82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.	

		Kontrola dostępu do stron internetowych 83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. 84. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 86. 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. 87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. 88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 89. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny. **Ochrona serwera plików** 95. Wsparcie dla systemów zaproponowanych przez	

		Wykonawcę w ofercie. 96. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 97. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 98. Wbudowana technologia do ochrony przed rootkitami i exploitami. 99. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 100. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 101. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 102. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 103. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 104. Możliwość skanowania dysków sieciowych i dysków przenośnych. 105. Skanowanie plików spakowanych i skompresowanych. 106. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.	

		107. Aplikacja powinna wspierać mechanizm klastrowania. 108. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 109. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 110. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 111. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 112. 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. 113. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 114. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 115. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 116. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 117. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.	

		118. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 119. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 120. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 121. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 122. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 123. 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. 124. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 125. Możliwość ręcznego wysłania próbki nowego	

		zagrożenia z katalogu kwarantanny do laboratorium producenta. 126. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 127. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 128. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 129. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. 130. Po instalacji systemu antywirusowego, 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. 131. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 132. System antywirusowy 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.	

		133. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 134. System antywirusowy 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. 135. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 136. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 137. Aplikacja musi wspierać skanowanie magazynu Hyper-V 138. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 139. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 140. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 141. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.	

		Administracja zdalna 105. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie. 106. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 107. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 108. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 109. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 110. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 111. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 112. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 113. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 114. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w	

		przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 115. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 116. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 117. 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. 118. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 119. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 120. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 121. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 122. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 123. Serwer administracyjny musi oferować	

		możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 124. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 125. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 126. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 127. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 128. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 129. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej. 130. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą	

		dedykowanej aplikacji. 131. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 132. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 133. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 134. 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. 135. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 136. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 137. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 138. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 139. Grupy dynamiczne 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. 140. 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. 141. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 142. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 143. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 144. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 145. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 146. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.	

		147. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 148. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 149. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 150. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 151. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 152. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 153. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 154. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 155. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie). 156. 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.	
23	Oprogramowanie biurowe	Pakiet biurowy musi zawierać co najmniej: a) Edytortekstów, b) Arkuszkalkulacyjny, c) Narzędzie do przygotowania i prowadzeniaprezentacji, d) Narządziedozarządzaniapocztąelektroniczną,kalendarzamiizadaniami Ogólne: a) Interfejs w językupolskim, b) wbudowana pomockontekstowa, c) możliwość instalacji na dostarczonym sprzęcie i systemieoperacyjnym Edytor tekstów: a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego), c) tworzenie szablonówdokumentów, d) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, e) wbudowana biblioteka obiektów graficznych isymboli, f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach, g) edycja nagłówków istopek, h) automatyczne numerowanie rozdziałów, tabel irysunków, i) automatycznetworzeniespisutreści,przypisówiodnośnik	

		ówdotekstu, j) śledzenie wprowadzonychzmian, k) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji), l) tworzenie korespondencjiseryjnej, m) tworzeniemakr, n) podgląd graficzny oraz wydrukdokumentów Arkusz kalkulacyjny: a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami), b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe orazczasowe, c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych iczasowych, d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje natabelach, e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D), f) formatowanie warunkowe komórekarkusza, g) śledzenie formuł oraz automatyczna weryfikacja ichpoprawności, h) tworzenie tabelprzestawnych, i) raporty z wykorzystaniem wyszukiwaniawarunkowego, j) automatyczne filtrowaniadanych, k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, bazdanych,	

		l) zapis wielu arkuszy w jednympliku, m) tworzenie szablonówdokumentów, n) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, o) tworzenie oraz edycji nagłówków istopek, p) osadzanie:symboli,tabel,rysunków,obiektówgraficznych orazwzorówmatematycznych, q) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji), r) tworzenie korespondencjiseryjnej, s) tworzeniemakr, t) podgląd graficzny oraz wydrukdokumentów, Narzędzie do przygotowania i prowadzenia prezentacji: a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami), b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego), c) tworzenie szablonówprezentacji, d) tworzenie animacji dla pojedynczych elementów jak i całychslajdów, e) wbudowana biblioteka obiektów graficznych isymboli, f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych orazfilmów), g) formatowanie tekstów, obiektów graficznych oraztabel, h) umieszczanie notatek oraz podkładudźwiękowego, i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracjidwumonitorowej),	

		j) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach, l) tworzenie oraz edycji nagłówków istopek, m) zabezpieczenie plików hasłem (zarówno do odczytu jakiedycji), n) podgląd graficzny oraz wydruk dokumentów (z możliwością wydruku kilku slajdów na jednej stronie oraznotatkami), Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami: a) pełna obsługa plików w formacie.pst, b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP, c) automatyczne filtrowaniepoczty, d) edycja i formatowanie tekstuwiadomości, e) tworzenie i obsługakatalogów, f) tworzenie szablonówdokumentów, g) tworzenie automatycznych reguł zarządzającychpocztą, h) oznaczanie wybranej poczty zdefiniowanymiatrybutami, i) importiobsługawielukalendarzy(wtymkalendarzyzdalnychwformacieiCal), j) udostępnianie kalendarza innymużytkownikom, k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawieniaprzypomnień), l) automatyczne wysyłanie i odbieranie informacji ospotkaniach,	

		m) tworzenie i zarządzaniezadaniami, n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrupodbiorców), o) odbiór i wysyłanie elektronicznych wizytówek w formacievCard, p) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, q) podgląd graficzny oraz wydrukdokumentów. Inne Licencja dożywotnia na pakiet biurowy Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe	
24	BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji:wersji BIOS wraz z datą; nr seryjnym komputera; ilości pamięciami RAM; typie procesora i jego prędkości; MAC adresu zintegrowanej karty sieciowej; unikalnych nr inwentarzowych tzw. Asset Tag'ów; nr seryjnym płyty głównej komputera Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość Wyłączania/Włączania technologii antykradzieżowej - Możliwość autentykacji użytkownika w BIOS z wykorzystaniem czytnika linii papilarnych - Możliwość konfiguracji pracy czujnika otwarcia obudowy w taki sposób aby przy próbie otwarcia obudowy komputera i	

		próbie jego uruchomienia pojawia się monit o podanie hasła supervisor'a zapisanego w BIOS. - Możliwość ustawienia hasła dla twardego dysku - Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, mikrofonu, zintegrowanej kamery, portów USB, Czytnika kart chipowych, bluetooth - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie Administratora oraz możliwość ustawienia takiej zależności, że widok użytkownika pozwala na podgląd ustawień, ale nie ma możliwości wprowadzania zmian w BIOS. - Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz trackpointa Możliwość ustawienia konieczności podania hasła Administratora przy próbie aktualizacji BIOS	
26.	Oprogramowanie dodatkowe	Oprogramowanie umożliwiające aktualizacje sterowników oraz podsystemu zabezpieczeń poprzez Internet. Oprogramowanie do wykonania kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku twardym, zewnętrznych dyskach, sieci, CD-ROM-ie oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego	

		reinstalacji. Oprogramowanie w wersji polskiej lub angielskiej.	
27.	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu - Certyfikat EPEAT na poziomie co najmniej GOLD. - ENERGY STAR 6.1 - Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z ww. systemem operacyjnym (wydruk ze strony Microsoft WHCL) - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	-
28.	Waga/Wymiary	Waga urządzenia z baterią podstawową max 2,5 kg, suma wymiarów urządzenia max 700 mm.	
29.	Szyfrowanie i bezpieczeństwo	Komputer wyposażony w moduł TPM 2.0 Notebook wyposażony w czujnik otwarcia obudowy zabezpieczający przed nieautoryzowanym dostępem do notebooka. Czujnik musi sygnalizować próbę nieautoryzowanego dostępu do wnętrza komputera. Praca czujnika konfigurowana z poziomu BIOS w ten sposób, że przy ustawionym haśle SUPERVISOR w przypadku nieautoryzowanego otwarcia obudowy hasło to będzie wymagane do podania przy próbie uruchomienia notebooka. Zamawiający uzna za równoważne dostarczenie linki zabezpieczającej typu Kensington zamykanej w taki sposób, że nie będzie możliwe otwarcie obudowy notebooka gdy linka zabezpieczająca zostanie umieszczona i zamknięta z wykorzystaniem kluczyka w dedykowanym slocie Kensington.	
30.	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą świadczona w miejscu użytkowania sprzętu (on-site) z	

		gwarantowanym czasem reakcji w następnym dniu roboczym.Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
31.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji. Możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
32.	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.11. Drukarka laserowa – 60 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)		Oferowana wartość parametru
1	Drukowanie	Szybkość drukowania w A4	40 str./min w mono	
		Czas pierwszego wydruku	Poniżej 4,5 sekund	
		Rozdzielczość	1200 x 1200 dpi	
		Języki druku	Emulacja PostScript3, PCL5e, PCL6 (XL), EPSON FX, IBM ProPrinter,	

			XPS, PDF(v1.7)	
		Czcionki drukarki	87 skalowanych czcionek PCL i 136 czcionek PostScript, 2 czcionki bitmapowe, OCR-A/B Czcionki rastrowe Czcionki Epson FX i IBM PPR o różnych rozmiarach	
		Dupleks	automatyczny	
2	Interfejs i oprogramowanie	Złącza	Port USB 2.0, Ethernet 10/100/1000	
		Kompatybilność z systemami operacyjnymi	Zaproponowanymi przez Wykonawcę w ofercie oraz z systemami posiadanymi przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10	
		Dodatkowe oprogramowanie	Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - funkcjonować w środowisku zaproponowanym przez Wykonawcę w ofercie; - obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB)	

			- podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; - możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; - podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów); - możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym.	
3	Podawanie papieru	Pojemność papieru	Podajnik 1: 250 arkuszy 80 g/m2; Podajnik uniwersalny: 100 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 Maksymalna pojemność	

			podajników: 880 arkuszy 80/m2	
		Format papieru	Podajnik 1: A4, A5, B5(JIS), A6, Letter, Legal 13, Legal 14, Executive, Statement; Podajnik 2: A4, A5, B5(JIS), Letter, Legal 13, Legal 14, Executive; Podajnik wielofunkcyjny: A4, A5, B5(JIS), A6, Letter, Legal 13, Legal 14, Executive, Statement, Koperty: Monarch, Com-9, Com-10, DL, C5, C6, 4 x 6", 5 x 7"; Druk dwustronny: A4, B5(JIS), Letter, up to Legal 14, Executive	
		Gramatura papieru	Podajnik 1/2: Od 60 do 120 g/m2; Podajnik uniwersalny: Od 60 do 163 g/m2; Druk dwustronny: Od 60 do 120 g/m2 Podajnik uniwersalny: 60 – 163 g/m2	
		Odbiornik papieru	Do 150 arkuszy stroną zadrukowaną do dołu Do 100 arkuszy stroną zadrukowaną do góry	
4	Pozostałe parametry techniczne:	Pamięć	Standardowa pamięć: 512 MB RAM, 3.0GB eMMC	
		Obciążenie	Maksymalne obciążenie do 80 000 stron miesięcznie	
5	Wymaganie	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą	

	dodatkowe:		gwarancji producenta drukarki	
		Wymagane dokumenty::	Certyfikat ISO 9001:2008 dla producenta oferowanego sprzętu. Certyfikat ISO 140001:2004 dla producenta oferowanego sprzętu.	
		Materiały eksploatacyjne:	Wymagana rozdzielność bębna i tonera.	
		Wydajność materiałów eksploatacyjnych	Urządzenie dostarczone z tonerem o wydajności 2000 str. zgodnie z ISO/ISC 19752. Urządzenie powinno mieć możliwość zastosowania tonerów o wydajności: 3 000 , 7 000 oraz 12000 stron zgodnie z ISO/ISC 19752.	
		Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem	

2.12. Urządzenie wielofunkcyjne A4 monochromatyczne (drukarka, skaner, kopiarka, fax) – 10 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Drukowanie	Szybkość drukowania- 33 str./min Szybkość druku dwustronnego- 18 str/min Czas pierwszego wydruku- 6,5 sekund	

		Rozdzielczość- 1200 x 1200 dpi Języki druku- PCL5e, PCL6, IBM-PPR, Epxon-FX,XPS Zespół drukowania- Dupleks mechaniczny	
2	Skanowanie	Rozdzielczość skanowania- 600 x 600 dpi Szybkość skanowania- Do 6 s/stronę w kolorze, 2s/stronę w czerni Głębia kolorów- Wejście 48 bit/Wyjście 24 bit Podawanie dokumentów- Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski Format- M-TIFF, PDF, XPS, JPEG, GIF, PNG Książka adresowa- LDAP, 300 adresów e-mail, 20 grup adresowych Skanowanie do- FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB,	
3	Kopiowanie	Czas wykonania pierwszej kopii- 10 sekund Szybkość kopiowania- do 33 kopii/min Rozdzielczość kopiowania- do 600 x 600dpi Zmniejszanie/powiększanie- Zoom 25-400% Maksymalna liczba kopii- 99	
4	Faksowanie	Złącza- RJ11 x 2 (Line/Tel), PSTN, Linia PBX Szybkość- ITU-T G3(Super G3) do 33,6kbps, do 2 s/str. Szybkie wybieranie- 16 przycisków szybkiego wybierania, 300 numerów Lista rozgłaszania- Maksimum 100 Pamięć stron- 4MB	
5	Interfejs i oprogramowanie	Złącza- Port USB 2.0, Ethernet 10/100/1000BaseTX Komunikacja bezprzewodowa- Tak, moduł bezprzewodowej karty sieciowej wbudowanej w urządzenie. Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie Dodatkowe oprogramowanie- Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje:	

		- funkcjonować w środowisku zaproponowanym przez Wykonawcę w ofercie; - obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT) - podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; - możliwość wpisania kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i nalepek; - podawać koszt przeprowadzonego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia, i przyznawanie im odpowiednich kosztów); - możliwość nakładania ograniczeń ilościowych na liczbę drukowanych stron oraz na koszty wydruku, w ujęciu dziennym, tygodniowym i miesięcznym. - Oprogramowanie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10	
6	Podawanie papieru	Pojemność papieru- Podajnik 1: 250 arkuszy 80 g/m2; Podajnik uniwersalny: 100 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 Format papieru- Podajnik 1: A4, A5, B5, A6 Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, Druk dwustronny: A4, B5 Gramatura papieru- Podajnik 1: 60 – 120 g/m2; Druk dwustronny: 60 – 120 g/m2; Podajnik uniwersalny: 60 – 120 g/m2	

		Podajnik skanera: 60 – 105 g/m2 Odbiornik papieru- Do 150 arkuszy stroną zadrukowaną do dołu	
7	Pozostałe parametry techniczne:	Pamięć (RAM)- Standardowa pamięć RAM: 512 MB Obciążenie- Maksymalne obciążenie do 60 000 stron miesięcznie	
8	Wymaganie dodatkowe:	Gwarancja- minimum36 miesięcy max zgodnie ze złożoną ofertą gwarancji producenta drukarki - naprawa w miejscu instalacji w ciągu 24h od daty zgłoszenia lub sprzęt zastępczy. Wymagane dokumenty: Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu Certyfikat ISO 140001:2004 producenta oferowanego sprzętu Materiały eksploatacyjne- Wymagana rozdzielność bębna i tonera. Toner startowy na 2 tys. stron zgodnie z normą ISO/ISC 19752 Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami) umożliwiającym wydruk przynajmniej 7 000 stron A4 przy pokryciu zgodnie z normą ISO/ISC 19752. Toner musi być tego samego producenta co drukarka, nie mogą być regenerowane.	
9	Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem	

2.13. Urządzenie wielofunkcyjne A4 kolorowe (drukarka, skaner, kopiarka, fax) – 10 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Drukowanie	Szybkość drukowania w A4- 26 str./min w kolorze, 30 str./min w mono Czas pierwszego wydruku- 9 sekund Rozdzielczość- 1200 x 600 dpi Czcionki druku- 87 skalowanych czcionek PCL i 80 czcionek PostScript Języki druku- PCL5c, PCL6, PostScript 3 (emulacja), IBM-PPR, Epxon-FX, XPS Zespół drukowania- Dupleks mechaniczny	
2	Skanowanie	Rozdzielczość skanowania- 60 x 600 dpi Szybkość skanowania- Do 26 str./min kolor, do 30 str./min w czerni Głębia kolorów- Wejście 30 bit/Wyjście 24 bit Podawanie dokumentów- Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski Format- M-TIFF, PDF, XPS, JPEG, Książka adresowa- LDAP lub 200 adresów e-mail i 20 grup adresowych Skanowanie do- FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB	
3	Kopiowanie	Czas wykonania pierwszej kopii- 14 sekund Szybkość kopiowania- Do 26 str./min kolor, do 30 str./min w czerni Rozdzielczość kopiowania- do 600 x 600dpi Zmniejszanie/powiększanie- Zoom 25-400% Maksymalna liczba kopii- 99	
4	Faksowanie	Złącza- RJ11 x 2 (Line/Tel), PSTN, Linia PBX Szybkość- ITU-T G3(Super G3) do 33,6kbps, do 3 s/str. Szybkie wybieranie- 16 przycisków szybkiego wybierania, 100 numerów Lista rozgłaszania- Maksimum 100 Pamięć stron- 250 MB	
5	Interfejs i oprogramowanie	Złącza- Port USB 2.0, Ethernet 10/100/1000BaseTX Kompatybilność z systemami operacyjnymi zaproponowanymi	

		przez Wykonawcę w ofercie; Dodatkowe oprogramowanie- Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - wymaga się aby aplikacja pracowała w środowisku zaproponowanym przez Wykonawcę w ofercie; - aplikacja powinna obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT), - aplikacja powinna rejestrować nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki; - aplikacja powinna rejestrować i w ramach raportów podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku; -aplikacja w zakresie modułu administracyjnego powinna pozwolić na indywidualne określenie kosztów materiałów eksploatacyjnych, oraz kosztu użycia zwykłej kartki, folii i innych nośników dla poszczególnych urządzeń lub grup urządzeń; - aplikacja powinna w zakresie funkcji raportowych podawać koszt zrealizowanego wydruku z możliwością rozróżnienia wydruków o małym i dużym pokryciu (wymagane jest rozróżnianie przynajmniej 5 różnych poziomów pokrycia); - w przypadku współpracy z urządzeniami kolorowymi w ramach funkcji ograniczenia dostępu aplikacja powinna mieć możliwość blokowania druku kolorowego (a w przypadku urządzeń wielofunkcyjnych kopii kolor) - aplikacja lub dostarczone urządzenia powinny mieć możliwość automatycznej konwersji drukowanych plików na postać czarno-biała dla użytkowników z założoną blokadą druku w kolorze; - aplikacja powinna umożliwić nałożenie ograniczeń ilościowych na	

		liczbę drukowanych stron w ujęciu dziennym, tygodniowym lub miesięcznym. - Oprogramowanie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10	
6	Podawanie papieru	Pojemność papieru- Podajnik 1: 250 arkuszy 80 g/m2; Podajnik uniwersalny: 100 arkuszy 80 g/m2; Podajnik skanera: 50 arkuszy 80 g/m2; Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 Format papieru- Podajnik 1: A4, A5, B5, A6 Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, nośniki (baner) do 130 cm długości Druk dwustronny: A4, B5, A5 Gramatura papieru- Podajnik 1: 64 – 176 g/m2; Druk dwustronny: 64 – 176 g/m2; Podajnik uniwersalny: 64 – 220 g/m2 Podajnik skanera: 60 – 105 g/m2 Odbiornik papieru- Do 150 arkuszy stroną zadrukowaną do dołu D0 100 arkuszy stroną zadrukowaną do góry	
7	Pozostałe parametry techniczne:	Pamięć (RAM)- Standardowa pamięć RAM: 1GB Szybkość procesora- 660 MHz Obciążenie- Maksymalne obciążenie do 45 000 stron miesięcznie	
8	Wymaganie dodatkowe:	Gwarancja- minimum36 miesięcy max zgodnie ze złożoną ofertą producenta drukarki. Wymagane dokumenty: Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy	

		serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu Certyfikat ISO 14001:2004 producenta oferowanego sprzętu Materiały eksploatacyjne- Wymagana rozdzielność bębna i tonera. Tonery startowe na 1 tys. stron (toner czarny i tonery kolorowe) zgodnie z normą ISO/ISC 19752 oraz normą ISO/IEC 19798. Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami).	
9	Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem	

2.14. Urządzenie wielofunkcyjne A3 monochromatyczne – 6 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Typ	Nabiurkowa lub wolnostojąca (połączony tryb czytniko-kopiarki)	
2	Maksymalny rozmiar oryginału	A3	
3	Rozmiary kopii	Kaseta 1, 3 i 4: A3, A4, A4R, A5R Format niestandardowy: 139,7–297 mm x 182–432 mm Kaseta 2: A3, A4, A4R, A5R, koperta (z opcjonalnym podajnikiem kopert D1) Podajnik ręczny: A3, A4, A4R, A5R, koperty Format niestandardowy: 99–297 mm x 148–432 mm	
4	Rozdzielczość	Odczyt:600 × 600 dpi Kopiowanie:600 × 600 dpi Drukowanie: 600 × 600 dpi, 1200 x 1200 dpi (tylko sterownik UFRII-	

		LT) Liczba tonów: 256 odcieni	
5	Prędkość kopii / druku	A4: 20 str. na minutę (tryb czarno-biały) A3: 15 str. na minutę (tryb czarno-biały)	
6	Powiększanie	Powiększenie: 25–400% Stałe: 25%, 50%, 70%, 100%, 141%, 200%, 400%	
7	Czas pierwszej kopii	Tryb czarno-biały: 6,4 s	
8	Czas rozgrzewania	30 s	
9	Wielokrotne kopie/wydruki	1–999	
10	Duplikowanie	Standard	
11	Wagi papieru	Kaseta: 64–90 g/m² Podajnik ręczny: 64–128 g/m² Druk dwustronny: 64–80 g/m²	
12	Pojemność papieru	Kaseta 1: 250 arkuszy (80 g/m²), Podajnik ręczny: 100 arkuszy (A4, A4R, A5; 80 g/m²), 50 arkuszy (A3; 80 g/m²) Opcjonalnie: 550 arkuszy x 2 kasety (80 g/m²) Całkowita pojemność: 2000 arkuszy	
13	Procesor	400 MHz	
14	Pamięć	256 MB	
15	Interfejs	Ethernet (100Base-TX/10Base-T), 1 port USB Host I/F 2.0, 1 port USB Device 1.0	
16	Źródło zasilania	220–240 V (prąd zmienny), 50/60 Hz, 3,3 A	
17	Wymiary	Suma wymiarów nie może przekraczać: 193 cm (z pokrywą szyby) Suma wymiarów nie może przekraczać: 203 cm (z podajnikiem DADF)	

18	Waga	Maksymalnie 52 kg	
19	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	
20	Inne	Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem	
21	Oprogramowanie	Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie oraz dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10; Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje: - wymaga się aby aplikacja pracowała w środowisku zaproponowanym przez Wykonawcę w ofercie; - aplikacja powinna obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT),	
22	Materiały eksploatacyjne	Toner startowy na 2 tys. stron zgodnie z normą ISO/ISC 19752 Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami).	

2.15. Tablet- 11 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Ekran	• Dotykowy • Rozdzielczość natywna nie mniejsza niż 1280x800 pikseli • Przekątna ekranu od 9 do 11 cali • Jasność co najmniej 600 nitów	
2	Procesor	Co najmniej 2 rdzenie, 1,5 Ghz	

3	Obudowa	• Posiadająca normę szczelności co najmniej IP67 • Powłoka dezynfekowana roztworem z zawartością alkoholu • Wytrzymująca upadek z min. 1,2 m	
4	Układ graficzny	Zintegrowany	
5	Pamięć RAM	Co najmniej 1GB	
6	Pamięć wewnętrzna	• Co najmniej 16GB • Możliwość rozszerzenia pamięci kartą typu MicroSD SDHC	
7	Bateria	Bateria typu „hot-swap" umożliwiająca wymianę baterii bez przerywania pracy urządzenia	
8	Czas pracy na baterii	Co najmniej 8h	
9	Temperatura pracy	Co najmniej -10 do nie więcej niż +50°C	
10	Komunikacja	• Wireless 802.11 a/b/g/n • Bluetooth 4.0 • GPS • 3G • Wbudowany czytnik kart HF RFID/NFC	
11	Czytnik kodów kreskowych	Wbudowany w urządzenie czytnik kodów kreskowych 1D i 2D	
12	Złącza	• Port ładowania i/lub multimedialny • USB i microUSB • Mini Jack 3.5mm	
13	System operacyjny	Zapewniający odpowiednią funkcjonalność dla systemu dostarczonego przez Wykonawcę	
14	Kamera	• Przednia co najmniej 1.2Mp • Tylna co najmniej 5.0Mp z auto-fokusem	
15	Inne	• Gwarancja- minimum36 miesięcy max zgodnie ze złożoną ofertą • Mikrofon, głośniki • Waga nie większa niż 970g • Urządzenie musi być zakupione w oficjalnym, polskim kanale	

		dystrybucyjnym	

2.16. Drukarka kodów paskowych – 5 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Rodzaj druku	Termiczna	
2	Rozdzielczość druku [dpi]	300dpi (12 pkt)	
3	Maksymalna długość druku	550 mm	
4	Minimalna długość druku	77 mm	
5	Prędkość druku [mm/s]	51 mm/sek	
6	Szerokość druku [mm]	19,05 mm, 25,4 mm, 30,16 mm	
7	Ilość pamięci FLASH	8 MB	
8	Ilość pamięci RAM	16 MB	
9	Dostępne interfejsy	USB oraz szeregowy	
10	Parametry środowiskowe	- Temperatura użytkowa: -40° do 60°C - Temperatura przechowywania: 0° do 21°C przy wilgotności względnej 35% do 50%	
11	Parametry	Uniwersalny zasilacz (zgodny z PFC) 100–240 V (AC), 50–60 Hz	

	elektryczne		
12	Wydruk kodów kreskowych	Kody liniowe: Codabar, Code 11, Code 39, Code 93, Code 128, EAN-8, EAN-13, EAN-14, GS1 DataBar™ (dawniej RSS), Industrial 2-of-5, Interleaved 2-of-5, Logmars, MSI, Plessey, Postnet, Standard 2-of-5, UPC-A, UPC-E, UPC-A i UPC-E z rozszerzeniami EAN 2- lub 5-cyfrowymi Dwuwymiarowe: Aztec Code, Codablock, Code 49, Data Matrix, MaxiCode, MicroPDF417, PDF417, QR Code	
13	Normy	Emisje: FCC część 15, punkt B, VCCI, C-Tick • Emisje i odporność: (CE): EN 55022 klasa B i EN 55024 • Bezpieczeństwo: CB Scheme IEC 60950-1:2001, TÜV NRTL • Zasilanie: IEC 60601-1:1995	
14	Gwarancja producenta	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.17. Skaner dowodów osobistych – 5 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Sensor CCD	24 bit/pixels-RGB, 8 bit/pixels (podczerwień) 450DPI	
2	Odczyt	Strefy MRZ z dowodu osobistego i paszportu Strefy VIZ z dowodu osobistego, prawo jazdy oraz karty studenckiej Kodów kreskowych: 1D- UPC-A, EAN8, EAN13, Code39, Code128, Interleaved 2 of 5 2D- PDF 417, Data Matrix, QR Code, Aztec Code ICAO 9303	
3	SDK	C/C++, C#, Visual Basic 6.0, VB.NET, Delphi Java	
4	Obsługiwane systemy operacyjne	Kompatybilne z zaproponowanymi przez Wykonawcę w ofercie oraz dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10 .	
5	Budowa	Brak części ruchomych	
6	Okno skanowania	4 mm szkło hartowane	

7	Interfejs	USB z odłączanym kablem komunikacyjnym	
8	Zabezpieczenia	Gniazdo Kensington	
9	Wymiary	Suma wymiarów nie może przekraczać (mm): 350	
10	Zasilanie	Poprzez port USB	
11	Sygnalizacja	Wizualna- 3 programowalne diody LED	
12	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.18. System Videorejestracja – e-tłumacz migowy 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Kamera	Przetwornik CMOS, 720p HD	
2	Przetwornik Mpix	4 Mpix	
3	Rozdzielczość	1280x800 , 30 klatek/sek.	
4	Zoom cyfrowy	4 - krotny	
5	Mikrofon	Mono wbudowany	
6	Złącze	USB 2.0	
7	Format	16:9 - panoramiczny	
8	Technologie	TrueColor, automatyczna korekta obrazu barwy I koloru dla zmiennego oświetlenia, plug&play , oprogramowanie do nagrywania I odtwarzania materiału wideo.	
9	Wsparcie dla Systemów	Kompatybilność dla systemów operacyjnych zaproponowanych przez Wykonawcę w ofercie.	
10	Głośniki	Stereo - 2 szt.	
11	Pasmo przenoszenia	50-17000 Hz	
12	Moc	większa od 8 W (RMS) na głośnik	

13	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.19. Karty Chipowe – 350 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Typ karty	Intelligentna chipowa , pojemność 256-Byte EEPROM	
2	Zabezpieczenie	Zabezpieczenie przed zapisem, programowany cod bezpieczeństwa (PSC) zabezpieczenie przed zapisem pierwszych 32 adresów (bajt 0 ... 31) pamięci danych	
3	Oranizacja pamięci	256 x8bit EEPROM, 32X1bit pamięć bezpiecznika	
4	Waga	Max. 66 g ± 5%	
5	Temperatura pracy	-40 / + 80 ° C dla chipa, -25 / + 80 ° C dla modułu	
6	Zasilanie	Napięcie zasilania 5 V+-10%	
7	Prąd zasilania	Max 3 mA (typowy 600 ěA)	
8	Czas wymazywania / zapisu EEPROM	Max . <5 ms	
9	Ochrona ESD typowa	Min 4.000 V	
10	EEPROM Trwałość	100 000 cykli wymazywania / zapisu	

	minimum wymazywania/ zapisu		
11	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.20. Skaner kodów kreskowych – 45 sztuk

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obsługiwane kody kreskowe	1D	
2	Dostępne interfejsy	USB, PS/2, RS-232	
3	Kabel komunikacyjny	USB	
4	Maksymalna odległość odczytu (cm)	43	
5	Technologia odczytu	Laser jednoliniowy	
6	Temperatura pracy	Od 0°C do 50°C	
7	Bezpieczny upadek na twardą powierzchnię (m)	1,5	

8	Sygnalizacja	Dźwiękowa oraz świetlna	
9	Wymagany kontrast kodu (%)	20	
10	Wymiary (cm)	Suma wymiarów nie może przekraczać 30 cm	
11	Temperatura składowania	Od -40°C do 70°C	
12	Dopuszczalna wilgotność otoczenia (%)	Od 5% do 95%	
13	Norma odporności (IP)	IP30	
14	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.21. Zestaw lekarza – diagnosty – 1 sztuka

2.21.1. Jednostka centralna lekarza – diagnosty – 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

Lp.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Komputer	Komputer będzie wykorzystywany dla potrzeb Systemu PACS. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu	
2	Obudowa	Typu Tower z obsługą kart PCI Express o wysokim profilu: 1x PCI Express 3.0 x16, 1 x PCI Express 3.0 x1 Wyposażona w min. 3 kieszenie: 1 szt. na napęd optyczny (dopuszcza się stosowanie napędów slim) zewnętrzna, 2 szt. 3,5”na standardowy dysk twardy, czytnik kart multimedialnych - Obudowa trwale oznaczona nazwą producenta, nazwą	

		komputera, numerem MTM, PN, numerem seryjnym;	
3	Chipset	Dostosowany do zaoferowanego procesora	
4	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, wyposażona w min. 3 porty SATAIII (6GB/s);	
5	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach stacjonarnych lub mobilnych, taktowany zegarem conajmniej 3,9 GHz, pamięcią cache CPU co najmniej 3 MB zapewniający wydajność CPU mierzoną przez PassMark Software na poziomie min. 5900 pkt. wynik dostepny na stronie http://www.cpubenchmark.net/	
6	Pamięć operacyjna	8 GB UDIMM, 2400MHz DDR4, 2 sloty na pamięć umożliwiające rozbudowę jednostki stacjonarnej do 32GB	
7	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
8	Napęd optyczny	Nagrywarka DVD +/-RW	
9	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4. Oraz druga zainstalowana medyczna karta graficzna dedykowana do współpracy z monitorami diagnostycznymi, posiadająca złącze: PCI-Express x16, posiadająca wyjścia: DisplayPort x 2 (Daisy chain supported), pamięć: 2GB, maksymalna pobierana moc: 26W	
10	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Konwersja 24bit DAC i 20bit ADC. Wsparcie dla 6 kanałowej DAC dla 16/20/24bit formatów PCM SNR dla DAC >98dBFSA SNR dla ADC >90dBFSA	
11	Karta sieciowa	10/100/1000 – złącze RJ45	

12	Porty/złącza	Wbudowane porty: - 1 x VGA, - 1 x DP, - 8 x USB w tym: 4x USB3.0 z przodu obudowy oraz 4x USB w tym min. 2 porty USB3.0 - port szeregowy COM, - port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim panelu - porty dźwiękowe z tyłu obudowy: wejście liniowe, wyjście liniowe oraz wejście mikrofonowe - czytnik kart pamięci 7-in-1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
13	Klawiatura/mysz	Klawiatura przewodowa w układzie US w kolorze zbliżonym do koloru obudowy. Mysz przewodowa (scroll) w kolorze zbliżonym do koloru obudowy	
14	Zasilacz	Zasilacz maksymalnie 180W o sprawności minimum 85%	
15	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia	

		aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".	

		17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i	

		przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN	

		e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
18	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - AssetTag, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego); Możliwość z poziomu Bios: - wyłączenia/włączania portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci	

		masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - 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 - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy	
19	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: - wykonanie testu pamięci RAM - test dysku twardego - test monitora - test magistrali PCI-e - test portów USB - test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: - PC: Producent, model - BIOS: Wersja oraz data wydania Bios - Procesor: Nazwa, taktowanie	

		- Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci - Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy - Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera	
20	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu - ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora w trybie IDLE 23 dB dołączyć dokument potwierdzający spełnienie wymagań Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	-
22	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock	-
24	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą świadczona w miejscu użytkowania sprzętu (on-site). Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
25	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
26	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.21.2. Monitor lekarza – diagnosty –2sztuki

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Matryca	IPS; przekątna: 21,3” / 54,1 cm; naturalna rozdzielczość: 1536 x 2048 (3:4); rozmiar wyświetlanego obrazu (W x S): 324,9 x 433,2 mm; rozmiar piksela: 0,2115 x 0,2115 mm; liczba kolorów: 10-bitowe kolory (DisplayPort): 1,07 miliarda (max.), 8- bitowe kolory: 16,77 miliona z palety 68 miliardów; kąty widzenia (pionowo / poziomo): 178° / 178°;	
2	Rodzaj podświetlenia	LED, jasność: 1000 cd/m2, rekomendowana jasność do kalibracji: 500 cd/m2, kontrast: 1500:1, czas reakcji (typowy): 25 ms (on/off)	
3	Sygnał wideo	Wejścia sygnałowe: DVI-D (dual link) x 1, DisplayPort x 1, wejścia sygnałowe (loop through): DisplayPort x 1 (do połączeń szeregowych), cyfrowa częstotliwość odświeżania: 31 – 127 kHz / 29 – 61,5 Hz w trybie synchronizacji klatek: 29,5 – 30,5 Hz, 59 – 61 Hz	
4	USB	Funkcje: 1 upstream, 2 downstream, standard 2.0.	
5	Zasilanie	Zasilacz: AC 100 – 120V, 200-240V : 50/60 Hz; maksymalny pobór mocy: 90W; Typowy pobór mocy: 50W; w trybie oszczędzania energii: mniej niż 1; zarządzenie energią: DVI DMPM, DisplyPort 1.2a	
6	Dodatkowe funkcje	Stabilizator jasności: TAK; Predefiniowany tryb pracy: CAL Switch; Digital Uniformity Equalizer: TAK	
7	Certyfikaty i standardy	CE (dyrektywa dotycząca wyrobów medycznych), EN60601-1, ANSI/AAMI ES60601-1, CSA C22.2 No. 601-1, IEC60601-1, VCC-B, FCC-B, Canadian ICES-003-B, RCM, RoHS, China RoHS, WEEE, CCC, EAC	

8	Akcesoria	Kabel zasilający, kabel sygnałowy dual-link (DVI-D – DVI-D), kabel sygnałowy (DisplayPort – DisplayPort), kabel USB, płyta z oprogramowaniem, instrukcja obsługi, podręcznik instalacji, instrukcja obsługi	
9	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą	

2.21.3. Monitor lekarza – diagnosty – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Matryca	Powłoka matrycy o wykończeniu matowym	
2	Przekątna ekranu	min. 21,5”;	
3	Nominalna rozdzielczość	rozdzielczość nie mniejsza niż: FHD (1920 x 1080);	
4	Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i min. 178 stopni w poziomie	
5	Plamka	Wielkość plamki (pojedyńczego piksela) maksymalna – 0.248 mm	
6	Gamut RGB	Nie mniejsza niż 72% RGB	
7	Kontrast	Kontrast wyświetlacza nie mniejszy niż: 1000:1	
8	Jasność	Jasność wyświetlacza nie mniejsza niż 250 cd/m^2	
9	Porty/złącza	Minimalna ilość dostępnych złącz w monitorze: 1 x DP, 1 x HDMI, 1 x D-SUB (VGA), 4 x USB 3.0	
10	Kable/przejściówki	Do monitora producent dołącza minimum kable: VGA o długości min. 1,8m, DP o długości min. 1,8m	
11	Stopa/Podstawa monitora	Musi umożliwiać: przechylenie w pionie min. 35 stopni (-5 / 30)	
12	Obudowa	- musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)	

		- Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością bez narzędziowego demontażu stopy. - Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora - Funkcja Pivot Obudowa trwale oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikacje zaoferowanego monitora	
13	Bezpieczeństwo	Złącze typu Kensington Lock	
14	Zasilacz	Zasilacz wewnętrzny/zewnętrzny max 65W	
15	Zużycie energii	- Maksymalne zużycie energii nie może przekraczać: 55 W - Zużycie energii w trypie uśpienia nie może przekraczać 0,5 W	
16	Certyfikaty i standardy	Certyfikat EPEAT na poziomie co najmniej GOLD. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony www.epeat.net, ENERGY STAR 6.0, ISO 9241-307, Certyfikat TCO, Deklaracja RoHS	
17	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą gwarancji producenta	
18	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji na stronie producenta modelu monitora - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta	

2.22. Zestaw technika – 1 sztuka

2.22.1. Jednostka centralna technika – 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

Lp.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Komputer	Komputer będzie wykorzystywany dla potrzeb Systemu PACS. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu	
2	Obudowa	Typu Tower z obsługą kart PCI Express o wysokim profilu: 1x PCI Express 3.0 x16, 1 x PCI Express 3.0 x1 Wyposażona w min. 3 kieszenie: 1 szt. na napęd optyczny (dopuszcza się stosowanie napędów slim) zewnętrzna, 2 szt. 3,5”na standardowy dysk twardy, czytnik kart multimedialnych - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym;	
3	Chipset	Dostosowany do zaoferowanego procesora	
4	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, wyposażona w min. 3 porty SATAIII (6GB/s);	
5	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach stacjonarnych lub mobilnych, taktowany zegarem co najmniej 3,9 GHz, pamięcią cache CPU co najmniej 3 MB zapewniający wydajność CPU mierzoną przez PassMark Software na poziomie min. 5900 pkt. wynik dostępny na stronie http://www.cpubenchmark.net/	
6	Pamięć operacyjna	4 GB UDIMM, 2400MHz DDR4, 2 sloty na pamięć umożliwiające rozbudowę jednostki stacjonarnej do 32GB	
7	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY	

		umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
8	Napęd optyczny	Nagrywarka DVD +/-RW	
9	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4.	
10	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Konwersja 24bit DAC i 20bit ADC. Wsparcie dla 6 kanałowej DAC dla 16/20/24bit formatów PCM SNR dla DAC >98dBFSA SNR dla ADC >90dBFSA	
11	Karta sieciowa	10/100/1000 – złącze RJ45	
12	Porty/złącza	Wbudowane porty: - 1 x VGA, - 1 x DP, - 8 x USB w tym: 4x USB3.0 z przodu obudowy oraz 4x USB w tym min. 2 porty USB3.0 - port szeregowy COM, - port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim panelu - porty dźwiękowe z tyłu obudowy: wejście liniowe, wyjście liniowe oraz wejście mikrofonowe - czytnik kart pamięci 7-in-1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
13	Klawiatura/mysz	Klawiatura przewodowa w układzie US w kolorze zbliżonym do koloru obudowy. Mysz przewodowa (scroll) w kolorze zbliżonym do koloru obudowy	

14	Zasilacz	Zasilacz maksymalnie 180W o sprawności minimum 85%	
15	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).	

		11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.	

		22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach	

		katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
18	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - AssetTag,	

		- MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego); Możliwość z poziomu Bios: - wyłączenia/włączania portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - 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 - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy	
19	Zintegrowany System	Wizualny system diagnostyczny producenta działający nawet w	

	Diagnostyczny	przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: - wykonanie testu pamięci RAM - test dysku twardego - test monitora - test magistrali PCI-e - test portów USB - test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: - PC: Producent, model - BIOS: Wersja oraz data wydania Bios - Procesor: Nazwa, taktowanie - Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci - Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy - Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera	
20	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu - ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora w trybie IDLE 23 dB dokument potwierdzający spełnienie wymagań Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	-

22	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock	-
24	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą świadczona w miejscu użytkowania sprzętu (on-site). Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
25	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
26	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.22.2. Monitortechnika – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Matryca	Powłoka matrycy o wykończeniu matowym	
2	Przekątna ekranu	min. 21,5”;	
3	Nominalna rozdzielczość	rozdzielczość nie mniejsza niż: FHD (1920 x 1080);	
4	Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i min. 178 stopni w poziomie	
5	Plamka	Wielkość plamki (pojedyńczego piksela) maksymalna – 0.248 mm	
6	Gamut RGB	Nie mniejsza niż 72% RGB	
7	Kontrast	Kontrast wyświetlacza nie mniejszy niż: 1000:1	
8	Jasność	Jasność wyświetlacza nie mniejsza niż 250 cd/m^2	

9	Porty/złącza	Minimalna ilość dostępnych złącz w monitorze: 1 x DP, 1 x HDMI, 1 x D-SUB (VGA), 4 x USB 3.0	
10	Kable/przejściówki	Do monitora producent dołącza minimum kable: VGA o długości min. 1,8m, DP o długości min. 1,8m	
11	Stopa/Podstawa monitora	Musi umożliwiać: przechylenie w pionie min. 35 stopni (-5 / 30)	
12	Obudowa	- musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) - Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością bez narzędziowego demontażu stopy. - Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora - Funkcja Pivot Obudowa trwale oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikacje zaoferowanego monitora	
13	Bezpieczeństwo	Złącze typu Kensington Lock	
14	Zasilacz	Zasilacz wewnętrzny/zewnętrzny max 65W	
15	Zużycie energii	- Maksymalne zużycie energii nie może przekraczać: 55 W - Zużycie energii w trypie uśpienia nie może przekraczać 0,5 W	
16	Certyfikaty i standardy	Certyfikat EPEAT na poziomie co najmniej GOLD. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony www.epeat.net, ENERGY STAR 6.0, ISO 9241-307, Certyfikat TCO, Deklaracja RoHS	
17	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą gwarancji producenta	
18	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji na stronie producenta modelu monitora - możliwość weryfikacji na stronie producenta	

		posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta	

2.23. Zestaw do duplikatora – 1 sztuka

2.23.1. Jednostka centralna – 1 sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

Lp.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Komputer	Komputer będzie wykorzystywany dla potrzeb Systemu PACS. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu	
2	Obudowa	Typu Tower z obsługą kart PCI Express o wysokim profilu: 1x PCI Express 3.0 x16, 1 x PCI Express 3.0 x1 Wyposażona w min. 3 kieszenie: 1 szt. na napęd optyczny (dopuszcza się stosowanie napędów slim) zewnętrzna, 2 szt. 3,5”na standardowy dysk twardy, czytnik kart multimedialnych - Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym;	
3	Chipset	Dostosowany do zaoferowanego procesora	

4	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, wyposażona w min. 3 porty SATAIII (6GB/s);	
5	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach stacjonarnych lub mobilnych, taktowany zegarem co najmniej 3,9 GHz, pamięcią cache CPU co najmniej 3 MB zapewniający wydajność CPU mierzoną przez PassMark Software na poziomie min. 5900 pkt. wynik dostępny na stronie http://www.cpubenchmark.net/	
6	Pamięć operacyjna	4 GB UDIMM, 2400MHz DDR4, 2 sloty na pamięć umożliwiające rozbudowę jednostki stacjonarnej do 32GB	
7	Dysk twardy	Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
8	Napęd optyczny	Nagrywarka DVD +/-RW	
9	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4.	
10	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Konwersja 24bit DAC i 20bit ADC. Wsparcie dla 6 kanałowej DAC dla 16/20/24bit formatów PCM SNR dla DAC >98dBFSA SNR dla ADC >90dBFSA	
11	Karta sieciowa	10/100/1000 – złącze RJ45	
12	Porty/złącza	Wbudowane porty: - 1 x VGA, - 1 x DP, - 8 x USB w tym: 4x USB3.0 z przodu obudowy oraz 4x USB w tym min. 2 porty USB3.0 - port szeregowy COM,	

		- port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim panelu - porty dźwiękowe z tyłu obudowy: wejście liniowe, wyjście liniowe oraz wejście mikrofonowe - czytnik kart pamięci 7-in-1 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
13	Klawiatura/mysz	Klawiatura przewodowa w układzie US w kolorze zbliżonym do koloru obudowy. Mysz przewodowa (scroll) w kolorze zbliżonym do koloru obudowy	
14	Zasilacz	Zasilacz maksymalnie 180W o sprawności minimum 85%	
15	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku	

		poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość	

		zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między	

		aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach	

		42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń	
18	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - AssetTag, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego); Możliwość z poziomu Bios: - wyłączenia/włączania portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1.użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej	

		- ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - 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 - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy	
19	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: - wykonanie testu pamięci RAM - test dysku twardego - test monitora - test magistrali PCI-e - test portów USB - test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: - PC: Producent, model - BIOS: Wersja oraz data wydania Bios - Procesor: Nazwa, taktowanie - Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci - Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy - Monitor: producent, model, rozdzielczość System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera	

20	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu - ENERGY STAR 6.1 - Deklaracja zgodności CE - Głośność jednostki mierzona z pozycji operatora w trybie IDLE 23 dB dołączyć dokument potwierdzający spełnienie wymagań Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki	-
22	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock	-
24	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą świadczona w miejscu użytkowania sprzętu (on-site). Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
25	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
26	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.23.2. Monitor – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Matryca	Powłoka matrycy o wykończeniu matowym	

2	Przekątna ekranu	min. 21,5”;	
3	Nominalna rozdzielczość	rozdzielczość nie mniejsza niż: FHD (1920 x 1080);	
4	Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i min. 178 stopni w poziomie	
5	Plamka	Wielkość plamki (pojedyńczego piksela) maksymalna – 0.248 mm	
6	Gamut RGB	Nie mniejsza niż 72% RGB	
7	Kontrast	Kontrast wyświetlacza nie mniejszy niż: 1000:1	
8	Jasność	Jasność wyświetlacza nie mniejsza niż 250 cd/m^2	
9	Porty/złącza	Minimalna ilość dostępnych złącz w monitorze: 1 x DP, 1 x HDMI, 1 x D-SUB (VGA), 4 x USB 3.0	
10	Kable/przejściówki	Do monitora producent dołącza minimum kable: VGA o długości min. 1,8m, DP o długości min. 1,8m	
11	Stopa/Podstawa monitora	Musi umożliwiać: przechylenie w pionie min. 35 stopni (-5 / 30)	
12	Obudowa	- musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) - Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością bez narzędziowego demontażu stopy. - Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora - Funkcja Pivot Obudowa trwale oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikacje zaoferowanego monitora	
13	Bezpieczeństwo	Złącze typu Kensington Lock	
14	Zasilacz	Zasilacz wewnętrzny/zewnętrzny max 65W	
15	Zużycie energii	- Maksymalne zużycie energii nie może przekraczać: 55 W - Zużycie energii w trypie uśpienia nie może przekraczać 0,5 W	

16	Certyfikaty i standardy	Certyfikat EPEAT na poziomie co najmniej GOLD. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony www.epeat.net, ENERGY STAR 6.0, ISO 9241-307, Certyfikat TCO, Deklaracja RoHS	
17	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą producenta	
18	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji na stronie producenta modelu monitora - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta	

2.24. Duplikator DVD – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Szybkość publikowania (nagrywanie i drukowanie):	Prędkość nagrywania i zadrukowywania płyt CD- 30 nośników wydruku na godzinę (tryb szybki); Prędkość nagrywania i zadrukowywania płyt DVD- 15 nośników wydruku na godzinę (tryb szybki)	
2	Tryb publikowania (liczba kopii):	Zewnętrzne wyjście: 5 nośników wydruku; wydajność: 50 nośników wydruku; Tryb wsadowy: 100 nośników wydruku	
3	Dane techniczne	Prędkość druku: 65 nośników wydruku na godzinę (tryb szybki);	

	drukowania	kierunek drukowania: dwukierunkowo, jednokierunkowo	
4	Rozdzielczość drukowania	1,440 DPI x 720 DPI (tryb szybki), 1,440 DPI (tryb wysokiej jakości); konfiguracja dysz: 180 dysz czarnych, 180 dysz na kolor	
5	Wkład atramentowy	Typ tuszu: Tusz Dye; kolory: Cyjan,, Magenta, Żółty, Jasny cyjan, Jasna Magenta, czarny; liczba kolorów: 6	
6	Powierzchnia obszaru drukowania	Standardowe ustawienia średnicy zewnętrznej: 116 mm; zakres ustawienia średnicy zewnętrznej: 119 mm – 70 mm; Standardowe ustawienia średnicy wewnętrznej: 50 mm – 18 mm; gwarantowana powierzchnia obszaru drukowania: 45 mm – 116 mm	
7	Napędy CD	Liczba napędów: 2; szybkość zapisywania: DVD-R 12x, CD-R 40x; Typy nośników wydruku: CD-R, DVD-R, DVD+R, DVD-R DL, DVD+R DL	
8	Obsługiwane nośniki	Wielkość średnicy zewnętrznej: 120 mm; Wielkość średnicy wewnętrznej: 15 mm; wymiar grubości: 1 mm	
9	Kompatybilne systemy operacyjne	z zaproponowanymi przez Wykonawcę w ofercie	
10	Wyposażenie	Pojedyncze wkłady atramentowe, instrukcja montażu, oprogramowanie (CD), kabel USB, instrukcja obsługi (CD)	
11	Złącza	USB 3.0	
12	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.25. Serwer PACS– 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 4U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych	

2	Procesor	Architektura x86. Zainstalowany procesor minimum 4C i częstotliwości 2.6GHz	
3	Liczba procesorów	Min. 1	
4	Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje	
5	Pamięć operacyjna	Zainstalowane min 16GB pamięci RAM Minimum 12 slotów na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Obsługa do 768GB pamięci operacyjnej potwierdzona w dokumentacji producenta dostępnej na oficjalnej stronie www producenta w dniu składania ofert. Pamięć o częstotliwości min. 2666MHz	
6	Zabezpieczenie pamięci	ECC, advanced ECC, mirroring, sparing	
7	Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz; 1 port DB-15 video (z tyłu obudowy).	
8	Dyski	W chwili dostawy serwer powinien umożliwiać zainstalowanie do 8 dysków 3.5" Hot Swap bez konieczności instalacji jakichkolwiek dodatkowych komponentów. Zainstalowanych 5 dysków 6TB oraz jeden dysk SSD o pojemności min 480GB	
9	Rozbudowa dysków	Możliwość instalacji dysków SED	
10	Kontroler dyskowy	Zainstalowany sprzętowy kontroler 12 Gb SAS/SATA z możliwością obsługi RAID 0/1/ 5/50/6/60 posiadający min 2GB pamięci cache umożliwiający implementacje technologii FastPath. Możliwość instalacji co najmniej dwóch kontrolerów.	
11	Zasilacz	Dwa zasilacze o mocy min: 750 W (200-240V) typu Platinum oraz dwa przewody zasilające c13-14 o długości min 1.5m	
12	Interfejsy sieciowe	Zintegrowane na płycie 2 porty RJ-45 Gigabit Ethernet 1000BASE-T.	

		Dodatkowy jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.	
13	Dodatkowe napędy	Możliwość instalacji napędów DVD-ROM, DVD-RW. Obsługa napędu RDX oraz LTO. W momencie dostawy serwer powinien posiadać zainstalowany napęd LTO6 wraz z kompletem 6 sztuk taśm LTO6.	
14	Dodatkowe porty	- z przodu obudowy: 1x USB 2.0 , 1xUSB 3.0 - z tyłu obudowy: 2x USB 3.0, 4xUSB 2.0, 1x DB-15 video, 1x RJ-45 do karty zarządzającej, 2x RJ-45 GbE porty sieciowe, - Wewnątrz obudowy: 1x USB 3.0 Wymagana możliwość instalacji portu DB-9 serial	
16	Chłodzenie	Dostępne 4 wentylatory; Dostępna redundancja minimum N+1	
17	Zarządzanie	Wraz z serwerem powinno być dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarządzenie infrastruktura serwerów, przełączników i storage bez udziału dedykowanego agenta, - przedstawianie graficznej reprezentacji zarządzanych urządzeń, - możliwość skalowania do minimum 560 urządzeń, - udostępnianie szybkiego podgląd stanu środowiska, - udostępnianie podsumowania stanu dla każdego urządzenia, - tworzenie alertów przy zmianie stanu urządzenia, - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5, - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania,	

		- definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń, - definiowanie roli użytkowników oprogramowania, - obsługa REST API, - obsługa SNMP, SYSLOG, Email Forwarding, - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - wsparcie dla NIST 800-131A oraz FIPS 140-2 - obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników, - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych, -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych, - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsługa NTP - Możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, - przesyłanie alertów do konsoli firm trzecich	
18	Funkcje zabezpieczeń	Hasło włączania, hasło administratora, dwa moduły TPM(Trusted Platform Modules)	
19	Urządzenia hot swap	Dyski twarde, zasilacze oraz wentylatory	
20	Obsługa	Możliwość wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych	
21	Diagnostyka	Panel diagnostyczny na froncie obudowy w postaci wyświetlacza	

		LED. Serwer musi być wyposażony w system diod LED na płycie głównej wskazujących awarie komponentów takich jak: kości pamięci, procesory, wentylatory. Możliwość włączenia diody identyfikującej serwer zarówno lokalnie jak i poprzez system zdalnego zarzadzania.	
22	Systemy operacyjne	Zainstalowany system operacyjny (SSO) musi posiadać następujące, wbudowane cechy: • Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1 TB pamięci RAM i dysku o pojemności min. 64 TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. • Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.	

		Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Graficzny interfejs użytkownika. • Zlokalizowane w języku polskim co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz	

		aktualizowania systemu. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.	
24	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą serwisu producenta on-site w trybie NBD Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku.	
25	Dodatkowe funkcjonalności:	Możliwość instalacji 2 kart GPU	
26	Dodatkowe	Przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry	

2.26. Przełącznik 16 portowy – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Architektura sieci LAN	GigabitEthernet	
2	Liczba portów 1000BaseT (RJ45)	16 sztuk	
3	Liczba gniazd MiniGBIC (SFP)	4 sztuki	
4	Porty komunikacji	RJ45 serial console port	
5	Zarządzanie,	RMON - Remote Monitoring, SNMP - Simple Network Management	

	monitorowanie i konfiguracja	Protocol, zarządzanie przez przeglądarkę WWW, Telnet	
6	Protokoły uwierzytelniania i kontroli dostępu	RADIUS - zdalne uwierzytelnianie użytkowników, SSL - Secure Sockets Layer	
7	Obsługiwane protokoły i standardy	Auto Negotiation, IEEE 802.1D - Spanning Tree, IEEE 802.1p – Priority, IEEE 802.1Q - Virtual LANs, IEEE 802.1s - Multiple Spanning Tree, IEEE 802.1w - Rapid Convergence Spanning Tree, IEEE 802.3 - 10BaseT, IEEE 802.3ab - 1000BaseT, IEEE 802.3ad - Link Aggregation Control Protocol, IEEE 802.3i 10BASE-T Ethernet, IEEE 802.3x - Flow Control, IEEE 802.3z - 1000BaseSX/LX, IEEE 802.1AB - Link Layer Discovery Protocol, DiffServ, IEEE 802.1x - Network Login, Port Mirror, NTP - Network Time Protocol, DHCP - Dynamic Host Configuration Protocol, FTP - protokół transmisji plików, IPv6, ACL - Access Control List, Port isolation, IGMP snooping, BPDU - Bridge Protocol Data Unit, Jumbo frame support	
8	Algorytm przełączenia	Storage-and-Forward	
9	Prędkość magistrali wewnętrznej	40 GB/s	
10	Przepustowość	29,8 mpps	
11	Bufor pamięci	4,1 MB	
12	Warstwa przełączenia	2	
13	Typ obudowy	1U Rack	
14	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	

2.27. Zasilacz UPS – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Moc	Urządzenie musi posiadać moc pozorną minimum 1700 VA; Urządzenie musi posiadać moc czynną minimum 1350W.	
4	Architektura	Urządzenie musi być wykonany w topologii line interactive VI z automatyczną regulacją napięcia AVR i czystym sinusoidalnym przebiegiem napięcia	
5	Obudowa	Zasilacz UPS musi posiadać uniwersalną obudowę Tower/Rack i być dostarczony wraz z kompletem kabli, dodatkowym modułem baterii oraz zestawem szyn do montażu w szafie Rack dla zasilacza UPS i modułu baterii	
	Czas przełączenia na pracę bateryjną	2-6 ms	
6	Parametry wejściowe	Napięcie znamionowe: 230 V (1-fazowe); Tolerancja napięcia 161– 276V +/- 4% ; Częstotliwość : 50 / 60 Hz (ustawiana automatycznie); Gniazdo IEC320 C14 (10A	
7	Parametry wyjściowe:	Napięcie znamionowe: 230 V (1-f) +/- 5% ; Częstotliwość :50 /60 Hz + /- 0,1 %; Współczynnik mocy 0,9 przy 1500 VA; Gniazda wyjściowe: 8 szt. IEC320 C13 (10A) (2 segmenty); Gniazdo dla dodatkowych kart komunikacyjnych; Gniazdo do podłączenia dodatkowej baterii	
8	Bateria	1. hermetyczne, bezobsługowe akumulatory 3 szt. x 12V/9 Ah o żywotności 5 lat wg klasyfikacji EUROBAT umieszczone wewnątrz UPS-a i zapewniające całkowity czas podtrzymania minimum 3 minut dla obciążenia 1350W, 5 minut dla obciążenia 1100W oraz 13 minut dla 550W; 2. Urządzenie musi mieć możliwość dodania 2 szt. dodatkowych modułów baterii każdy wyposażony w 9 szt. akumulatorów 12V/7 Ah. Dodatkowy moduł baterii wydłuża czas podtrzymania do 13 minut dla obciążenia 1350W. Dwa dodatkowe moduły baterii wydłużają czas podtrzymania do 24 minut dla obciążenia 1350W;	

		3. Urządzenie musi mieć czas ładowania baterii < 4 godz. do pojemności użytkowej 80 % wydajności po całkowitym rozładowaniu; 4. Zasilacz UPS musi mieć możliwość wymiany akumulatory przez użytkownika	
9	Urządzenie musi posiadać wyświetlacz LCD z ikonami graficznymi wskazującymi:	obciążenie obecne, poziom obciążenia, alarm ogólny, awaria baterii/ wymiana baterii, przeciążenie, pojemność baterii, tryb normalny/ praca z użyciem baterii, automatyczna regulacja napięcia włączona, wyjścia programowalne, wartość na wejściu	
11	Zasilacz UPS musi posiadać alarmy dźwiękowe sygnalizujące:	tryb bateryjny, przeciążenie, konieczność wymiany baterii	
12	Wyposażenie	1. Urządzenie musi posiadać port USB i RS232 oraz możliwość dodania karty komunikacyjnej WEB / SNMP (v1 & v3, IP v4 & v6) lub karty ze stykami bezpotencjałowymi; 2. Wraz z zasilaczem UPS musi zostać dostarczone oprogramowanie do monitorowania i wyłączania stacji roboczych działające w systemach operacyjnych zaproponowanych przez Wykonawcę w ofercie oraz karta SNMP, która gwarantuje połączenie z siecią Ethernet 10/100 Mb i jest wyposażona w złącze RJ45. Oprogramowanie musi obsługiwać platformy wirtualne; 3. Urządzenie musi posiadać możliwość ochrony linii danych: tłumik udarowy NTP: RJ45 10 Base T; 4. Urządzenie musi posiadać wyłącznik awaryjny EPO	
13	Zasilacz UPS musi	Bezpieczeństwo: IEC/EN 62040-1, AS 62040.1.1, AS 62040.1.2;	

	być zgodny z Normami	Kompatybilność elektromagnetyczna IEC/EN 62040-2, AS 62040.2; Certyfikaty: RoHS, CE, RCM (E2376);	
14	Zasilacz UPS musi spełniać parametry środowiskowe co najmniej takie jak :	Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C); Wilgotność: 95 % bez kondensacji; Poziom hałasu w odległości 1 m < 50 dB	
16	Inne	Urządzenie musi mieć możliwość dodania ręcznego bezprzerwowego bypassu serwisowego typu HOT SWAP z gniazdami IEC 320 C13 tego samego producenta co zasilacz UPS.	
17	Gwarancja	Urządzenie musi być objęte gwarancja producenta na okres minimum 36 miesięcy maximum zgodnie ze złożoną ofertą na moduł elektroniki oraz akumulatory	

2.28. Skaner CR – 1sztuka

Producent / Model oferowanego sprzętu lub oprogramowania _____

L.p.	Parametr	Charakterystyka (wymagania minimalne)	Oferowana wartość parametru
1	Dostępne płyty i kasety	Płyty obrazowe ST-VI: 35 X 43cm (14” X 17”), 35 X 35cm (14” X 14”), 10” X 12”, 8” X 10”, 24 X 30cm, 18 X 24cm, 15 X 30cm Kasety IP : 35 X 43cm (14” X 17”), 35 X 35cm (14” X 14”), 10” X 12”, 8” X 10”, 24 X 30cm, 18 X 24cm, 15 X 30cm	

2	Czas oczekiwania na załadowanie kasety	Min. 49 sekund	
3	Wydajność przetwarzania	do 47 kaset/godz.	
4	Parametry odczytu	10 pikseli/mm, 5 pikseli/mm	
5	Czas wyświetlenia na monitorze	Min. 33 sek.	
6	Ilość pojemników na film	1	
7	Sieć	10 Base T/100 Base TX	
8	Zasilanie	Jednofazowe 50-60Hz; AC120-240V ±10% 2A (max)	
9	Środowisko pracy	Temperatura: 15-30°C; Wilgotność: 15-80%RH (bez kondensacji); Ciśnienie atmosferyczne: 750-1060hPa	
10	Zestaw rozruchowy	kaseta + płyta ST-VI: 35 X 43cm- 2 szt., 24 X 30cm- 2 szt., 18x24cm- 2 szt.	
11	Wyposażenie	Stolik, uchwyt na kasety 2 sztuki, stolik monitorowy	
11	Gwarancja	Minimum 36 miesięcy maximum zgodnie ze złożoną ofertą.	