Plik należy podpisać elektronicznie za pomocg kwalifikowanego podpisu elektronicznego lub podpisu zaufanego lub elektronicznego podpisu osobistego przez osobę/osoby uprawniong/-ne do składania oświadczeń woli w imieniu Wykonawcy.

Załącznik nr 3 do SWZ CUW.PK.343.20.2024

UWAGA: Załącznik składany razem z ofertą

Opis przedmiotu zamówienia/*formularzu opisu oferowanego sprzętu*

„Dostawa sprzętu komputerowego i urządzeń peryferyjnych w ramach utworzenia i wsparcia funkcjonowania Branżowego Centrum Umiejętności w dziedzinie przemysłu meblarskiego w Zespole Szkół im. M. Rataja w Reszlu" – postępowanie II dla części dostawa sprzętu komputerowego

1. Sprzęt komputerowy

1. **Komputer stacjonarny – 9 zest.**			
L.p.	Nazwa parametru	**Opis wymagań minimalnych (wszystkie parametry nie gorsze niż i/lub równoważne)**	**Opis Wykonawcy dotyczący oferowanego sprzętu: parametry, producent, typ, model i in. stosownie do treści wiersza** (wypełnić pola z komentarzami, pola z napisem „opis", odpowiednio przekreślić spełnia/nie spełnia) nie wypełniać pól przekreślonych
Komputer stacjonarny - 9 zest. **Zastosowanie:** Oprogramowanie Autodesk Fusion 360, Autodesk AutoCAD.			
1.	Typ	Komputer stacjonarny. Wymagane jest podanie modelu, symbolu oraz producenta	Producent: Model:…… Symbol:……
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna	
3.	Wydajność obliczeniowa	Procesor osiągający w teście CPU PassMark wynik min. 32 000 punktów według wyników ze strony http://www.cpubenchmark.net	Producent:…….. Model:……..
4.	Pamięć operacyjna RAM	Min. 32GB DDR5 MHz non-ECC możliwość rozbudowy do min 128GB, min. cztery sloty na pamięć RAM.	*Opis:* ……
5.	Parametry pamieci	512GB SSD PCIe	*Opis:* ……

	masowej	Komputer musi umożliwiać instalację min 3 HDD, dopuszcza się konfigurację dysk M.2 + 2 dyski magnetyczne	
6.	Wydajność grafiki	Karta graficzna niezintegrowana z własną pamięcią min. 12GB GDDR6. Osiągająca w teście Pas-smark G3D Mark wynik co najmniej 14 000 punktów według wyników ze strony www.videocardbenchmark.net. Złącza min. HDMI oraz DisplayPort.	Producent:……. Model:…….
7.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. audio out. Czytnik kart multimedialnych czytający min. karty SD 4.0	
8.	Obudowa	Typu Mini Tower z obsługą kart wyłącznie o pełnej wysokości. Umożliwiająca montaż 2 x dysku 3.5" lub 2 x dysków 2.5" wewnątrz obudowy. Możliwość instalacji napędy optycznego w dedykowanej wnęce zewnętrznej 5.25" typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji piono-wej. Suma wymiarów obudowy nieprzekraczająca 980 mm. Zasilacz o mocy min. 750W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 92% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 89% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, Wydruki 80plus musza być potwierdzone przez producenta. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5" oraz 2,5" bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisk POWER [tzn. barw i miganie] W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię CMOS baterii, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.	
9.	Zgodność z	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami	(jako potwierdzenie poprawnej współpracy

	systemami operacyjnymi	operacyjnymi (jako potwierdzenie poprawnej współpracy **Wykonawca dołączy do oferty** dokument Producenta oprogramowania w postaci wydruku potwierdzający certyfikację rodziny produktów).	**Wykonawca dołączy do oferty** dokument Producenta oprogramowania w postaci wydruku potwierdzającego certyfikację rodziny produktów.)
10.	Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.	
11.	Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: ▪ monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; ▪ zdalną konfigurację ustawień BIOS, ▪ zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; ▪ zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/).	
12.	Wirtualizacja	Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).	

13.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne], - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego], Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej Możliwość włączenia/wyłączenia kontrolera SATA w tym również pojedynczo, Możliwość włączenia/wyłączenia kontrolera audio, Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [musi umożliwiać znaki specjalne (@#$%^)] Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.	
14.	Certyfikaty i standardy	Certyfikat ISO9001, ISO50001 dla producenta sprzętu Deklaracja zgodności CE Certyfikat TCO, wymagana certyfikacja na stronie: http://tco.brightly.se/pls/nvp/!tco_search Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta	

		jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram	
15.	Warunki gwarancji Wsparcie Techniczne	Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. Sposób realizacji usług wsparcia technicznego : ▪ Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. ▪ Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera	**wymagane dołączenie do oferty oświadczenia potwierdzonego**, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta

		Serwisowego Producenta – **wymagane dołączenie do oferty oświadczenia potwierdzonego**, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta 3 lata świadczona w miejscu użytkowania sprzętu (on-site)	
16.	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".	Producent:……. Nazwa oprogramowania:…….

		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	
17.	Oprogramowanie zabezpieczające	System chroniący przed zagrożeniami. Silnik musi umożliwiać co najmniej: • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci, • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.	Producent:…… Nazwa oprogramowania:……..

		• Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Szyfrowanie danych: • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej	

		platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1.Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 2.Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: •różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie •funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD	

		•funkcje regulowania połączeń WiFi i Bluetooth •funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe •funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi •funkcje blokowania dostępu dowolnemu urządzeniu •możliwość tymczasowego dodania dostępu do urządzenia przez administratora •zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu •możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka •możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora •możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry •możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich •funkcję wirtualnej klawiatury •możliwość blokowania każdej aplikacji •możliwość zablokowania aplikacji w oparciu o kategorie •możliwość dodania własnych aplikacji do listy zablokowanych •zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze •dodawanie innych aplikacji •dodawanie aplikacji w formie portable •możliwość wyboru pojedynczej aplikacji w konkretnej wersji •dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB •kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool •możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. •możliwość zablokowania funkcji Printscreen •funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx •funkcje monitorowania i kontroli przepływu poufnych informacji •możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików •możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj •możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe	

		•ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe •ochrona zawartości schowka systemu •ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL •możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych •ochrona plików zamkniętych w archiwach •Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem •możliwość tworzenia profilu DLP dla każdej polityki •wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania •ochrona przez wyciekiem plików poprzez programy typu p2p Monitorowanie zmian w plikach: •Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. •Funkcje monitorowania określonych rodzajów plików. •Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. •Generator raportów do funkcjonalności monitora zmian w plikach. •możliwość śledzenia zmian we wszystkich plikach •możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach •możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: •usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku •optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem •możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich •instruktaż stanowiskowy pracowników Zamawiającego •dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: 1.Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) 2.Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) 3.Mac OS X, Mac OS 10 4.Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat Platforma do zarządzania z poziomu systemów Android i iOS: •Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę •Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem	

		•Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email •Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika •Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi •Musi posiadać możliwość eksportu danych użytkownika Zarządzanie urządzeniem •Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO •Musi umożliwiać import listy urządzeń z pliku CSV •Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych •Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta •Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał •Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres •Musi zawierać podgląd aktualnie zainstalowanych aplikacji •Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, •Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł •Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1.Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2.Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3.Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge	

		- Mozilla Firefox - Google Chrome - Safari 4.Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5.Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6.Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych - Deduplikacja danych, - Backup przyrostowy i różnicowy, - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, - Backup danych lokalnych – plikowy oraz poczty Outlook, - Backup otwartych plików (VSS), - Filtr plików oraz folderów, - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), - Wyłączanie komputera po wykonaniu backupu, - Przywracanie danych do wskazanej lokalizacji, - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, - Wyszukiwanie plików w repozytorium użytkownika, Ustawienia - Automatyczne logowanie, - Zapamiętywanie danych logowania, - Automatyczne uruchamianie programu przy starcie systemu, - Ustawianie priorytetu dla procesu backupu,	

		- Zmiana klucza szyfrującego, - Ustawienia przepustowości/zajętości pasma, - Konfiguracja wydajności procesu backupu, Bezpieczeństwo - Zastępowanie nazwy pliku GUID-em, - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, - Kompresja danych, - Transmisja po bezpiecznym protokole TLS, - Deklaracja klucza szyfrującego dane użytkownika, - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, - Obliczanie sumy kontrolnej, - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług serwisowych oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.	
18.	Wymagania dodatkowe	Wbudowane porty: 2x DisplayPort (obsługujące zintegrowaną kartę graficzną) 1x LAN 10/100/1000 wspierająca obsługę WoL (funkcja włączana przez użytkownika), umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem. Porty USB min : Panel przedni 2x USB 3.2 Typ-A 2x USB 3.2 Typ-C Panel Tylny: 2x USB 3.2 typ-A 2x USB 2.0 typ-A 2x USB 3.2 Typ-C Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB TYP-A i TYP-C nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować	

		instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową (wlutowane w laminat płyty głównej). Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla oferowanego urządzenia; wyposażona w : • 1 gniazdo PCIe x16 piątej generacji pełnej wysokości • 1 gniazdo PCIe x4 trzeciej generacji pełnej wysokości • 1 gniazdo PCIe x4 czwartej generacji pełnej wysokości • 4 złącza UDIMM z obsługą do 128GB DDR4 pamięci RAM, • 3 złącza SATA w tym 2 szt SATA 3.0; • 1 złącze M.2 dedykowane dla syków SSD • 1 złącze M.2 WLAN Klawiatura USB w układzie polski programisty Mysz laserowa USB z rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.	
19.	Dodatkowe oprogramowanie	Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające : - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji : a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej	

		instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.	
20.	Monitor	Wielkość Min. 23,8" Powłoka matrycy: Matowa Rodzaj matrycy: LED, IPS Typ ekranu: Płaski Rozdzielczość ekranu 1920 x 1080 (FullHD) Format obrazu 16:9 Częstotliwość odświeżania ekranu min. 100 Hz Kontrast statyczny min. 1300:1 Technologia ochrony oczu Redukcja migotania (Flicker free) Wbudowane głośniki min. 2x2W Filtr światła niebieskiego Złącza: HDMI, DisplayPort Regulacja kąta pochylenia (Tilt): Tak w sumie min. 24 stopnie Dołączone akcesoria: Zasilacz Kabel HDMI	Producent:…… Model:……

2. **Komputerów All In One Typ I – 11 zest.**			
L.p.	Nazwa parametru	**Opis wymagań minimalnych** **(wszystkie parametry nie gorsze niż i/lub równoważne)**	**Opis Wykonawcy dotyczący oferowanego sprzętu:** **parametry, producent, typ, model i in. stosownie do treści wiersza** (wypełnić pola z komentarzami, pola z napisem „opis", odpowiednio przekreślić spełnia/nie spełnia) nie wypełniać pól przekreślonych
1.	**Komputer stacjonarny All In One Typ I**, w którym podzespoły komputerowe takie jak: płyta główna, procesor czy układ graficzny zostały umieszczone w jednej obudowie z ekranem w taki sposób, który uniemożliwia odłączenie komputera od monitora, posiadający wspólny system zasilania. **- 11 zest.** **Zastosowanie:** Oprogramowanie Autodesk Fusion 360, Autodesk AutoCAD.		Producent: ……. Model: ……
2.	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 umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. 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-810H.	Spełnia / nie spełnia
3.	Ekran	Przekątna: min 27" Rozdzielczość: min. QHD(2560x1440), 350nits, format 16:9, kontrast 1000:1, kąty widzenia 178°, matryca matowa wykonana w technologii WVA/MVA/IPS/PLS	*Opis:* ……
4.	Obudowa	– musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) – zintegrowana z monitorem (AIO) – założona linka kensington musi jednocześnie umożliwiać przypięcie AIO do biurka oraz zabezpieczenie obudowy przed nieautoryzowanym otwarciem	Spełnia / nie spełnia

		– podstawa musi umożliwiać regulację kąta nachylenia w zakresie –5° do przodu oraz 20° do tyłu, wysokości w zakresie 110mm, pivot 90° oraz swivel +/- 45° – Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością beznarzędziowego demontażu stopy. Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnym, PN pozwalającym na jednoznaczna identyfikacje zaoferowanej konfiguracji	
5.	Chipset	Dostosowany do zaoferowanego procesora	Spełnia / nie spełnia
6.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera umożliwiająca konfigurację wielodyskową min. SATAIII + M.2 PCIe	Spełnia / nie spełnia
7.	Procesor	Procesor posiadający min. 16 rdzeni osiągający w teście CPU PassMark wynik min. 37200 punktów według wyników ze strony http://www.cpubenchmark.net	Producent:…… Model:……..
8.	Pamięć operacyjna	Min. 16GB DDR5 5600Mhz z możliwością rozszerzenia do 64 GB Ilość banków pamięci: min. 2 szt.	*Opis:* ……
9.	Dysk twardy	Min. 1TB SSD M.2 PCIe NVMe OPAL oraz zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	*Opis:* ……
10.	Napęd optyczny	Wbudowana Nagrywarka DVD +/-RW	Spełnia / nie spełnia
11.	Karta graficzna	Dedykowana karta graficzna z własną pamięcią min. 6GB GDDR6, osiągająca minimalną ilość 14 500 punktów w uśrednionym teście Passmark, według wyników ze strony https://www.videocardbenchmark.net	Producent:…… Model:……..
12.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo 2 x 5W, wbudowane dwa mikrofony, wbudowana kamera o rozdzielczości 5MP z wbudowaną mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery, kamera obsługująca Windows Hello	*Opis:* ……
13.	Porty/złącza	Wbudowane (minimum): DisplayPort out,1 x HDMI IN 1.4/OUT 2.1 TMDS, 7 x USB 3.2 (z czego jeden umożliwiający szybkie ładowanie urządzeń zewnętrznych/podłączanych nawet przy wyłączonym komputerze), czytnik kart multimedialnych, 1 x RJ 45 (LAN), 1 x wyjście na słuchawki i mikrofon (Combo), Wśród portów USB wymaga się, aby przynajmniej jeden port był w standardzie Thunderbolt 4. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	*Opis:* ……
14.	Klawiatura/mysz	Klawiatura przewodowa w układzie US. Mysz przewodowa z rolką (scroll)	Spełnia / nie spełnia
15.	Karta sieciowa	Port sieci LAN 100/1000 Ethernet RJ 45 zintegrowany z płytą główną. Zainstalowana wewnątrz obudowy bezprzewodowa karta sieciowa dwuzakresowa WiFi AC 2x2 + Bluetooth 5.1	Spełnia / nie spełnia

16.	Zasilacz	Energooszczędny zasilacz o mocy minimalnej 225W oraz sprawności min. 90%.	*Opis:* .....
17.	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	Producent:…… Model:……..

		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, - Numer inwentarzowy, - MAC Adres karty sieciowej, - wersja i data BIOS - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM, - stanie pracy wentylatora - informacja o licencji na system operacyjny **Możliwość z poziomu Bios:** - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy oraz z boku obudowy. - wyłączenia karty sieciowej (WIFI i LAN), karty audio, mikrofonu, kamery, czytnika kart multimedialnych - możliwość wyłączenia wirtualizacji w BIOS - możliwość zaprogramowania automatycznego włączenia komputera o określonej porze - możliwość ustawienia następujących haseł: hasła administratora, hasła Power-On, hasła na dysk twardy	Spełnia / nie spełnia

		- dostęp do systemu logowania zdarzeń w BIOS. System musi zapewniać logowanie co najmniej takich zdarzeń jak: update BIOS, zmiany w konfiguracji, wyczyszczenie logów - 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 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 • 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 System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	Spełnia / nie spełnia
20.	Certyfikaty i standardy	Dla producenta sprzętu: – Certyfikat ISO 9001 dla producenta sprzętu – Certyfikat ISO 14001 dla producenta sprzętu – Certyfikat ISO 50001 dla producenta sprzętu Urządzenie musi spełniać: – Deklaracja zgodności CE – TCO 9.0 – TCO Edge – Zgodność z dyrektywą RoHS – TÜV Rheinland Low Blue Light	Spełnia / nie spełnia
21.	Waga/rozmiary	Waga urządzenia wraz ze stopą max. 11 kg	Spełnia / nie spełnia

	urządzenia		
22.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.	Spełnia / nie spełnia
23.	Bezpieczeństwo	Złącze typu Kensington Lock Moduł dTPM 2.0 Wbudowana mechaniczna zasłona kamery	Spełnia / nie spełnia
24.	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.	Producent:…… Model:……..
25.	Oprogramowanie zabezpieczające– w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	System chroniący przed zagrożeniami. Silnik musi umożliwiać co najmniej: • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci, • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.	Producent:…… Model:……..

		• Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Szyfrowanie danych: • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem	

		docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmurę: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:	

		• różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi • funkcje blokowania dostępu dowolnemu urządzeniu • możliwość tymczasowego dodania dostępu do urządzenia przez administratora • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx • funkcje monitorowania i kontroli przepływu poufnych informacji • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych	

		typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przez wyciekiem plików poprzez programy typu p2p Monitorowanie zmian w plikach: • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • Funkcje monitorowania określonych rodzajów plików. • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • Generator raportów do funkcjonalności monitora zmian w plikach. • możliwość śledzenia zmian we wszystkich plikach • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach • możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich • instruktaż stanowiskowy pracowników Zamawiającego • dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: 1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) 2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) 3. Mac OS X, Mac OS 10 4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat	

		Platforma do zarządzania z poziomu systemów Android i iOS: • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • Musi posiadać możliwość eksportu danych użytkownika Zarządzanie urządzeniem • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO • Musi umożliwiać import listy urządzeń z pliku CSV • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres • Musi zawierać podgląd aktualnie zainstalowanych aplikacji • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu	

		zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych - Deduplikacja danych, - Backup przyrostowy i różnicowy, - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, - Backup danych lokalnych – plikowy oraz poczty Outlook, - Backup otwartych plików (VSS), - Filtr plików oraz folderów, - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),	

		- Wyłączanie komputera po wykonaniu backupu, - Przywracanie danych do wskazanej lokalizacji, - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, - Wyszukiwanie plików w repozytorium użytkownika, Ustawienia - Automatyczne logowanie, - Zapamiętywanie danych logowania, - Automatyczne uruchamianie programu przy starcie systemu, - Ustawianie priorytetu dla procesu backupu, - Zmiana klucza szyfrującego, - Ustawienia przepustowości/zajętości pasma, - Konfiguracja wydajności procesu backupu, Bezpieczeństwo - Zastępowanie nazwy pliku GUID-em, - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, - Kompresja danych, - Transmisja po bezpiecznym protokole TLS, - Deklaracja klucza szyfrującego dane użytkownika, - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, - Obliczanie sumy kontrolnej, - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług serwisowych oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.	
26.	Warunki Gwarancji Wsparcie Techniczne	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera ▪ Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. ▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera	**wymagane dołączenie do oferty oświadczenia potwierdzonego**, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta

		▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-17:00 Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. min. 3 lata świadczona w miejscu użytkowania sprzętu (on-site) Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – **wymagane dołączenie do oferty oświadczenia potwierdzonego**, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta	

3. K**omputer All In One Typ II – 2 zest.**			
L.p.	Nazwa parametru	**Opis wymagań minimalnych** **(wszystkie parametry nie gorsze niż i/lub równoważne)**	**Opis Wykonawcy dotyczący oferowanego sprzętu:** **parametry, producent, typ, model i in. stosownie do treści wiersza** (wypełnić pola z komentarzami, pola z napisem „opis", odpowiednio przekreślić spełnia/nie spełnia) nie wypełniać pól przekreślonych
1.	**Komputer stacjonarny All In One Typ II**, w którym podzespoły komputerowe takie jak: płyta główna, procesor czy układ graficzny zostały umieszczone w jednej obudowie z ekranem w taki sposób, który uniemożliwia odłączenie komputera od monitora, posiadający wspólny system zasilania **- 2 zest.** **Zastosowanie:** Oprogramowanie Autodesk Fusion 360, Autodesk AutoCAD.		Producent:…….. Model: ……..
2.	Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora.	
3.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza	

		danych, stacja programistyczna	
4.	Wydajność obliczeniowa	Procesor osiągający w teście CPU PassMark wynik min. 32 000 punktów według wyników ze strony http://www.cpubenchmark.net	Producent:…… Model:……
5.	Pamięć RAM	Min. 16GB DDR4 3200MHz możliwość rozbudowy do 64GB RAM.	*Opis:* ……
6.	Pamięć masowa	Min. 512GB SSD Możliwość instalacji dodatkowego dysku twardego M.2 lub 2.5	*Opis:* ……
7.	Wydajność grafiki	Karta graficzna niezintegrowana, z własną pamięcią, osiągająca w teście wydajności G3D Mark wynik min. 7800 punktów według wyników ze strony www.videocardbenchmark.net	Producent:…… Model:……
8.	Matryca	Min. 23,8”, plamka max. 0,275mm	
9.	Rozdzielczość	FHD (1920x1080)	
10.	Jasność typowa	min. 250 cd/m²	
11.	Kontrast	700:1	
12.	Barwa koloru (typowa)	72% NTSC	
13.	Kąty Horizontal/Vertical	178(+/- 89) / 178 (+/-89)	
14.	Rodzaj matrycy	Matowa IPS	
15.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP z diodą LED informującą użytkownika o pracy. Mechaniczna chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy). Wbudowane w obudowę dwa mikrofony.	
16.	Obudowa	Typu All-in-One zintegrowana z monitorem min. 23.8 cali. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędz. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100, Suma wymiarów obudowy z zainstalowanym standem nie może przekraczać: 114cm Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 94cm Zasilacz wewnętrzny o mocy min. 200W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia	

		lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa jednostki typu All – in – One musi umożliwiać: Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. Regulację wysokości w zakresie minimum 10 cm.	
17.	Zdalne zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.: - Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; - Zdalną konfigurację ustawień BIOS, - Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; - Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. - Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/).	
18.	Bezpieczeństwo	Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS	
19.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty	

		głównej oraz w BIOS systemu.	
20.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne] - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej Możliwość włączenia/wyłączenia kontrolera SATA Możliwość włączenia/wyłączenia kontrolera audio, Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [musi umożliwiać znaki specjalne (@#$%^)] Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach: codziennie lub w wybrane dni tygodnia, Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.	
21.	Certyfikaty i standardy	• Certyfikat ISO9001 dla producenta sprzętu • Certyfikat ISO 50001 dla producenta sprzętu	

		• Deklaracja zgodności CE • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Certyfikat TCO – znajdujący się na stronie: http://tcocertified.com/product-finder/	
22.	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	Producent:…… Nazwa oprogramowania:……

		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	
23.	Wymagania dodatkowe	Wbudowane porty: 1 port wejściowy HDMI 1.4b (do 1920 x 1080 przy 60 Hz) 1 port wyjściowy HDMI 2.1 (do 4096 × 2160 przy 60 Hz) 1 złącze DisplayPort++ 1.4a (do 5120 x 3200 przy 60 Hz) 6 porty USB 3.2 Type-A 1 port wyjścia liniowego audio z możliwością przekonfigurowania Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp. Wszystkie porty dostępne dla użytkownika na krawędzi obudowy 1x Universal audio jack 1x One Line-out audio 1x RJ-45 port 10/100/1000 Mbps Czytnik kart SD 4.0 Karta WiFi 6ax + bluetooth 5.3 Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale	

		oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi Czytnik kart multimedialnych SD 4 Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)	
24.	Oprogramowanie zabezpieczające	System chroniący przed zagrożeniami. Silnik musi umożliwiać co najmniej: • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji, • wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, • stosowanie kwarantanny, • wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) • skanowanie urządzeń USB natychmiast po podłączeniu, • automatyczne odłączanie zainfekowanej końcówki od sieci, • skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach. • Musi posiadać moduł ochrony IDS/IPS • Musi posiadać mechanizm wykrywania skanowania portów • Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów • Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości Szyfrowanie danych: • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.	Producent:…… Nazwa oprogramowania:…….

		Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet. • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji Zarządzanie przez Chmurę:	

		1.Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach 2.Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3.Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur 4.Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5.Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach 6.Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 7.Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1.Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 2.Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi • funkcje blokowania dostępu dowolnemu urządzeniu • możliwość tymczasowego dodania dostępu do urządzenia przez administratora • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone,	

		iPad, iPod, Webcam, card reader, BlackBerry • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich • funkcję wirtualnej klawiatury • możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie • możliwość dodania własnych aplikacji do listy zablokowanych • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze • dodawanie innych aplikacji • dodawanie aplikacji w formie portable • możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • możliwość zablokowania funkcji Printscreen • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx • funkcje monitorowania i kontroli przepływu poufnych informacji • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe • ochrona zawartości schowka systemu • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • możliwość tworzenia profilu DLP dla każdej polityki • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przez wyciekiem plików poprzez programy typu p2p	

		Monitorowanie zmian w plikach: • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • Funkcje monitorowania określonych rodzajów plików. • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • Generator raportów do funkcjonalności monitora zmian w plikach. • możliwość śledzenia zmian we wszystkich plikach • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach • możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich • instruktaż stanowiskowy pracowników Zamawiającego • dokumentacja techniczna w języku polskim Wspierane platformy i systemy operacyjne: 1.Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit) 2.Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit) 3.Mac OS X, Mac OS 10 4.Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat Platforma do zarządzania z poziomu systemów Android i iOS: • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. Zarządzanie użytkownikiem • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • Musi posiadać możliwość eksportu danych użytkownika Zarządzanie urządzeniem	

		• Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO • Musi umożliwiać import listy urządzeń z pliku CSV • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres • Musi zawierać podgląd aktualnie zainstalowanych aplikacji • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: Wymagania dotyczące technologii: 1.Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2.Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3.Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5.Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6.Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy	

		operacyjne: - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 7. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych - Deduplikacja danych, - Backup przyrostowy i różnicowy, - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, - Backup danych lokalnych – plikowy oraz poczty Outlook, - Backup otwartych plików (VSS), - Filtr plików oraz folderów, - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), - Wyłączanie komputera po wykonaniu backupu, - Przywracanie danych do wskazanej lokalizacji, - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, - Wyszukiwanie plików w repozytorium użytkownika, Ustawienia - Automatyczne logowanie, - Zapamiętywanie danych logowania, - Automatyczne uruchamianie programu przy starcie systemu, - Ustawianie priorytetu dla procesu backupu, - Zmiana klucza szyfrującego, - Ustawienia przepustowości/zajętości pasma, - Konfiguracja wydajności procesu backupu, Bezpieczeństwo - Zastępowanie nazwy pliku GUID-em, - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,	

		- Kompresja danych, - Transmisja po bezpiecznym protokole TLS, - Deklaracja klucza szyfrującego dane użytkownika, - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, - Obliczanie sumy kontrolnej, - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług serwisowych oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.	
25.	Dodatkowe oprogramowanie	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale	

		czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania	
26.	Oprogramowanie biurowe	**Licencja MS Office Home & Business 2019 PL 64 bit lub w wersji nowszej lub oprogramowanie równoważne**, które musi spełniać minimalne poniższe wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1) Wymagania odnośnie interfejsu użytkownika: a) pełna polska wersja językowa interfejsu użytkownika, b) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 2) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz. U. 2017r, poz.2247). 3) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców; 4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy); 5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim; 6) Pakiet zintegrowanych aplikacji biurowych musi zawierać: a) edytor tekstów, b) arkusz kalkulacyjny, c) narzędzie do przygotowywania i prowadzenia prezentacji, d) narzędzie do tworzenia drukowanych materiałów informacyjnych, e) narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, f) kontaktami i zadaniami), g) narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie	Producent:……. Nazwa oprogramowania:……

		urządzenia typu tablet PC z mechanizmem OCR, 7) Edytor tekstów musi umożliwiać: a) edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty, b) wstawianie oraz formatowanie tabel, c) wstawianie oraz formatowanie obiektów graficznych, d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków, f) automatyczne tworzenie spisów treści, g) formatowanie nagłówków i stopek stron, h) śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie, i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, j) określenie układu strony (pionowa/pozioma), k) wydruk dokumentów, l) wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną, m) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013 i 2016, wykorzystywanych przez Zamawiającego, z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji, o) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem, p) wymagana jest dostępność do oferowanego edytora tekstu, bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem, przy pomocy certyfikatu kwalifikowanego, zgodnie z wymaganiami obowiązującego w Polsce prawa. 8) Arkusz kalkulacyjny musi umożliwiać: a) tworzenie raportów tabelarycznych,	

		b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, c) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, d) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), e) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych, f) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, g) wyszukiwanie i zamianę danych, h) wykonywanie analiz danych przy użyciu formatowania warunkowego, i) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, j) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, k) formatowanie czasu, daty i wartości finansowych z polskim formatem, l) zapis wielu arkuszy kalkulacyjnych w jednym pliku, m) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013 i 2016 wykorzystywanych przez Zamawiającego, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, n) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 9) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a) przygotowywanie prezentacji multimedialnych, b) prezentowanie przy użyciu projektora multimedialnego, c) drukowanie w formacie umożliwiającym robienie notatek, d) zapisanie jako prezentacja tylko do odczytu, e) nagrywanie narracji i dołączanie jej do prezentacji, f) opatrywanie slajdów notatkami dla prezentera, g) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i	

		wideo, h) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, i) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, j) możliwość tworzenia animacji obiektów i całych slajdów, k) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, l) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania Microsoft PowerPoint 2003, 2007, 2010, 2013 i 2016 wykorzystywanych przez Zamawiającego. 10) Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: a) tworzenie i edycję drukowanych materiałów informacyjnych, b) tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów, c) edycję poszczególnych stron materiałów, d) podział treści na kolumny, e) umieszczanie elementów graficznych, f) wykorzystanie mechanizmu korespondencji seryjnej, g) płynne przesuwanie elementów po całej stronie publikacji, h) eksport publikacji do formatu PDF oraz TIFF, i) wydruk publikacji, j) możliwość przygotowywania materiałów do wydruku w standardzie CMYK. 11) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, b) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców, c) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, d) automatyczne grupowanie poczty o tym samym tytule, e) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, f) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia,	

		g) zarządzanie kalendarzem, h) udostępnianie kalendarza innym użytkownikom, i) przeglądanie kalendarza innych użytkowników, j) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach, k) zarządzanie listą zadań, l) zlecanie zadań innym użytkownikom, m) zarządzanie listą kontaktów, n) udostępnianie listy kontaktów innym użytkownikom, o) przeglądanie listy kontaktów innych użytkowników, p) możliwość przesyłania kontaktów innym użytkowników.	
27.	Warunki gwarancji Wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. 3 lata świadczona w miejscu użytkowania sprzętu (on-site)	**wymagane dołączenie do oferty oświadczenia potwierdzonego**, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta

4. Urządzenie drukujące wielofunkcyjne – 1 szt.			
L.p.	Nazwa parametru	**Opis wymagań minimalnych** **(wszystkie parametry nie gorsze niż i/lub równoważne)**	**Opis Wykonawcy dotyczący oferowanego sprzętu: parametry, producent, typ, model i in. stosownie do treści wiersza** (wypełnić pola z komentarzami, pola z napisem „opis”, odpowiednio przekreślić: spełnia/nie spełnia) nie wypełniać pól przekreślonych)
Urządzenie drukujące wielofunkcyjne			Producent:…… Model:……..
1.	Funkcje urządzenia	Drukowanie, skanowanie, kopiowanie, faksowanie.	
2.	Technologia wydruku	atramentowa, kolorowa	
3.	System stałego zasilania atramentem (CIS)	TAK	
4.	Rozdzielczość wydruku	min. 4800 x 1200 dpi	
5.	Maksymalny format skanu	A4	
6.	Formaty wydruku	A4 A5 A6 B5 DL Letter	
7.	Szybkość wydruku	Min. 20 str. / minutę w kolorze Min. 30 str. / minutę w mono	
8.	Wydruk dwustronny	Automatyczny	
9.	Podajnik dokumentów	Automatyczny na min. 30 arkuszy, pozostały na min. 250 arkuszy	
10.	Dodatkowe wymagania	Tusz do samodzielnego napełniania (w zestawie atrament pozwalający na wydruk min. 13 000 stron w czerni oraz min. 5000 stron w kolorze)	
11.	Gwarancja	Producenta min. 36 miesięcy	

5. Monitor interaktywny / komputera OPS / – 1 zest.			
L.p.	Nazwa parametru	**Opis wymagań minimalnych (wszystkie parametry nie gorsze niż i/lub równoważne)**	**Opis Wykonawcy dotyczący oferowanego sprzętu: parametry, producent, typ, model i in. stosownie do treści wiersza** (wypełnić puste pola i pola z komentarzami, odpowiednio przekreślić: spełnia/nie spełnia) nie wypełniać pól przekreślonych)
monitor interaktywny / komputer OPS			Producent:…… Model:……
1.	Ekran	min. 65 cali, dotykowy, format 16:9, IPS	
2.	Rozdzielczość	Min. 3840 x 2160 UHD 4K	
3.	Jasność	min. 350 cd/m²	
4.	Czas reakcji	Max. 9ms	
5.	Kontrast	Statyczny min. 1200:1	
6.	Ilość punktów dotykowych	Min. 30 punktów	
7.	Głośniki	Wbudowany min. 2x15W	
8.	Złącza	Wbudowane min. 3x HDMI, 5x USB, 1x LAN, 1x mini jack	
9.	Typ komputera	OPS	
10.	Zastosowanie komputera	Kompatybilny z ekranem interaktywnym z pkt. 5.5. ppkt. 1.	
11.	Pamięć operacyjna komputera	Minimalna wymagana pojemność pamięci RAM 8 GB	*Opis:* ……
12.	Procesor komputera	Procesor osiągający w teście CPU PassMark wynik min. 10900 punktów według wyników ze strony http://www.cpubenchmark.net	Producent:…… Model:……
13.	Grafika komputera	Karta graficzna osiągająca w teście wydajności CPU PassMark wynik min. 2600 punktów według wyników ze strony http://www.cpubenchmark.net	Producent: …… Model:……
14.	Parametry pamięci masowej komputera	Dysk SSD min. 256 GB	*Opis:* ……
15.	Wyposażenie standardowe	W zestawie min. moduł wifi, 4 x rysik, kabel zasilający, kabel HDMI, kabel USB, pilot z bateriami, kabel zasilający	*Opis:* ……

5a. Statyw jezdny kompatybilny z monitorem interaktywnym z poz. 2.5) – 1 szt.		
Nazwa parametru	**Opis wymagań minimalnych (wszystkie parametry nie gorsze niż i/lub równoważne)**	Opis Wykonawcy dotyczący oferowanego sprzętu **Parametry, producent, typ, model i in. stosownie do treści wiersza** (wypełnić puste pola i pola z komentarzami, odpowiednio przekreślić: spełnia/nie spełnia) nie wypełniać pól przekreślonych)
Statyw jezdny kompatybilny z monitorem interaktywnym z poz. 5)		Producent:…… Model:……
1.	Min. statyw jezdny kompatybilny z monitorem interaktywnym, regulowany, półka szklana, waga bez monitora maks. 18kg	

4. Przedmiotem zamówienia jest:

1) sprzedaż i dostarczenie Sprzętu wraz z Oprogramowaniem
2) udzielenie przez Wykonawcę gwarancji i zapewnienie serwisu gwarancyjnego i wsparcia technicznego na dostarczony Sprzęt
3) udzielenie licencji na Oprogramowanie
4) dostarczenie przez Wykonawcę Dokumentacji dostarczonego Sprzętu

5. Termin dostawy

L.p.	Przedmiot dostawy	Liczba dostarczanego sprzętu, oprogramowania	Termin dostawy
Dostawa sprzętu komputerowego			
1.	Komputer stacjonarny, monitor, klawiatura, mysz.	9 zestawów	120 dni kalendarzowych od podpisania umowy
2.	Komputer All In One, klawiatura, mysz. Typ I	11 zestawów	
3.	Komputer All In One, klawiatura, mysz. Typ II	2 zestawy	
4.	Urządzenie drukujące wielofunkcyjne	1 sztuka	
5.	Monitor interaktywny/ komputer OPS/	1 zestaw	

5a	Statyw kompatybilny z monitorem interaktywnym z poz. 5	1 sztuka	

UWAGA: Nie podlega uzupełnieniu wypełniony przez Wykonawcę powyższy formularz opisu oferowanego sprzętu.

6. **Wymagania ogólne**

Numer wymagania	Opis wymagania
1.	Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych z zastrzeżeniem, że ich parametry techniczne, funkcjonalne i użytkowe nie mogą być gorsze niż wskazane w SWZ.
2.	W przypadku gdy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, parametry lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”
3.	Wskazane wyżej określenie przedmiotu zamówienia ma charakter wyłącznie pomocniczy w przygotowaniu oferty i ma na celu wskazać oczekiwane standardy co do minimalnych parametrów technicznych oczekiwanych materiałów. Przez ofertę równoważną należy rozumieć ofertę o parametrach technicznych, jakościowych, nie gorszych od opisu wskazanego przez zamawiającego w opisie przedmiotu zamówienia. Parametry wskazane przez zamawiającego są parametrami minimalnymi, granicznymi. Pod pojęciem „parametry” rozumie się funkcjonalność i jakość. W związku z powyższym zamawiający dopuszcza możliwość zaoferowania materiałów o innych znakach towarowych, patentach lub pochodzeniu, natomiast nie o innych właściwościach i funkcjonalnościach niż określone w niniejszym postępowaniu.
4.	W sytuacji, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art.101 ust. 1 pkt. 2 i ust. 3 ustawy Pzp, dopuszcza się rozwiązania równoważne opisanym.
5.	Wykonawca, który powołuje się na rozwiązania równoważne opisanym przez Zamawiającego, zobowiązany jest udowodnić w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104 -106 ustawy Pzp, że: a) Proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia; b) Dostawa spełnia wymagania dotyczące wydajności lub funkcjonalności określone przez Zamawiającego.
6.	Dla jednoznacznej identyfikacji oferowanego sprzętu należy podać nazwę producenta, a także nazwę i model oferowanego sprzętu. Zamawiający wymaga również podania faktycznych parametrów sprzętu, o którym mowa powyżej, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany sprzęt spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane urządzenia spełniają wymagania Zamawiającego.
7.	Wykonawca zobowiązuje się dostarczyć przedmiot zamówienia fabrycznie nowy, zakupiony w oficjalnym kanale sprzedaży producenta na rynek polski lub UE, nie będący uprzednio przedmiotem ekspozycji lub wystaw, wyprodukowany nie wcześniej niż w roku 2023, nie przewidziany przez producenta do wycofania z produkcji lub sprzedaży, wolny od wad fizycznych i prawnych, sprawny technicznie, nieuszkodzony, kompletny i gotowy do użytku, zgodnie z jego przeznaczeniem oraz spełniający wymagania określone w SWZ.
8.	Dostawa powinna zawierać komplet dokumentacji i instrukcji, karty gwarancyjne, również - niewyłączone i ograniczone czasowo licencje sporządzone w

	języku polskim na dostarczone oprogramowanie, listę numerów seryjnych i numerów produktu dostawy, wszystkie akcesoria i kable niezbędne do montażu i uruchomienia sprzętu w miejscu instalacji (w siedzibie Zamawiającego). Dopuszcza się wskazanie i udostępnienie bezpłatnie serwisu internetowego z aktualną dokumentacją i instrukcjami, o ile skorzystanie z nich przez Zamawiającego nie będzie związane z ponoszeniem przez Zamawiającego jakichkolwiek kosztów.
9.	Towar musi być dostarczony w oryginalnych opakowaniach fabrycznych producenta, oznakowanych etykietami zawierającymi: rodzaj i nazwę asortymentu, nazwę i adres producenta oraz numer fabryczny. Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające).
10.	Wykonawca zobowiązany jest ustalić z Zamawiającym dzień oraz godzinę dostawy uwzględniając godziny pracy Zamawiającego.
11.	Uszkodzony lub brakujący sprzęt Wykonawca dostarczy na koszt własny najpóźniej w kolejnym dniu roboczym. Towar niezgodny z Opisem Przedmiotu Zamówienia uznaje się za brakujący. Po przekroczeniu czasu wyznaczonego na realizację zadania do czasu dostarczenie towaru wolnego do wad oraz zgodnego z OPZ Wykonawca pozostaje w zwłoce i zostaną mu naliczone kary umowne zgodnie z zapisami zawartymi we wzorze umowy.
12.	Zamawiający wymaga udzielenia gwarancji jakości zgodnie z zapisem niniejszego załącznika oraz umowy. Szczegóły dotyczące gwarancji doprecyzowane zostały w projektowanych postanowieniach umowy stanowiących załącznik nr 4 do SWZ.

Plik należy podpisać elektronicznie za pomocą kwalifikowanego podpisu elektronicznego lub podpisu zaufanego lub elektronicznego podpisu osobistego przez osobę/osoby uprawnioną/-ne do składania oświadczeń woli w imieniu Wykonawcy.