SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

do postepowania prowadzonego w trybie przetargu nieograniczonego pn. „Zakup sprzętu komputerowego i oprogramowania na potrzeby projektu: Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym”

Przedmiotem zamówienia jest zakup i dostawa sprzętu komputerowego i oprogramowania spełniającego parametry określone w poniższej tabeli:

	Laptop z oprogramowaniem – 136 sztuk	
1	Ekran	TFT 15.6” LED IPS Full HD o rozdzielczości 1920 x 1080, z powłoką matową, nie dopuszcza się matryc typu "glare". Klapa komputera otwierana do 180 stopni.
2	Wydajność/ Procesor	Zaoferowany komputer powinien osiągać w teście wydajności BAPCO - MobileMark 2018 minimum: • Performance qualification na poziomie 1143, • Productivity na poziomie 1061, • Creativity na poziomie 1162, • Web browsing na poziomie 1210. Zamawiający wymaga, aby powyższy wynik osiągnięty był na komputerze o konfiguracji oferowanej. Test musi być przeprowadzony dla minimum trzech interakcji przy rozdzielczości wyświetlania obrazu nie mniejszej niż 1920x1080. **Zamawiający wymaga dołączenia do oferty wyniku testu przeprowadzonego na oferowanej konfiguracji komputera potwierdzającego osiągnięcie przez oferowany komputer wymaganego wyniku w postaci wydruku z przeprowadzonego testu (raport lub PrintScreen z wynikiem testu), potwierdzonego za zgodność z oryginałem przez Wykonawcę.**
3	Chipset	Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora.
4	Obudowa	Dopuszczalne kolory – czarny lub odcienie szarości. Wskaźniki diodowe (baterii oraz zasilania).
5	Pamięć RAM	1x 8GB DDR4 (pamięć RAM rozszerzalna do 32GB). 1 slot wolny.
6	Dysk twardy	1x 256 GB PCIe NVMe SSD (możliwość dołożenia drugiego dysku bez utraty gwarancji)
		Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów. Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.
7	Karta graficzna	Zintegrowana.
8	Karta dźwiękowa	Karta dźwiękowa zgodna z Intel High Definition Audio. Wbudowane dwa frontowe głośniki stereo oraz cyfrowy mikrofon.
9	Połączenia i karty sieciowe	Karta sieciowa LAN 10/100/1000 LAN (WOL Ready) WLAN 802.11a/b/g/n/acR2+ax wireless LAN wraz z Bluetooth 5.1 Technologia MU-MIMO 2x2 Wi-Fi 6 AX201
10	Porty/złącza (wbudowane)	1 x Złącze RJ-45 (podłączenie sieci lokalnej) ~~1 x Czytnik Kart pamięci SD™~~ 3 x USB 3.2 Gen 1 (w tym 1 szt. z możliwością ładowania urządzeń zewnętrznych przy wyłączonym laptopie) 1 x USB Type-C port (z możliwością ładowania urządzenia, wsparciem dla technologii DisplayPort over USB-C i wsparciem dla standardu Thunderbolt 4) 1 x VGA 1 x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo) 1 x HDMI 2.0 ze wsparciem HDCP 1 x port zasilania 1 x złącze Kensington
11	Klawiatura	Klawiatura z podświetleniem klawiszy. Pełnowymiarowa z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura musi być wyposażona w 2 klawisze ALT (prawy i lewy).
12	Urządzenie wskazujące	Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka posiadającą certyfikat Microsoft Precision Touchpad Certification.

13	Kamera	Wbudowana, o parametrach: - HD 1280 x 720 rozdzielczość - 720p HD audio/video nagrywanie. Wbudowana ruchoma osłona kamery.
15	Bateria	Czas pracy na baterii minimum 7 godzin i 27 minut potwierdzony przeprowadzonym testem MobileMark 2018 Battery Life (do oferty załączyć wydruk przeprowadzonego testu) Zasilacz o mocy min. 45W
16	Zasilacz	Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 45W wraz z przewodem zasilającym.
17	Waga i wymiary	Waga max do 2 kg z baterią.
18	Bezpieczeństwo	- Zabezpieczenie BIOS hasłem użytkownika. - Zintegrowany z płytą główną dedykowany 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 - Trusted Platform Module 2.0. - Czytnik linii papilarnych - Urządzenie spełniające normy MIL-STD 810G
19	Gwarancja PRODUCENTA	a) Gwarancja producenta komputera min 24 miesiące – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. b) Gwarancja na baterię min. 12 miesięcy. c) Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie producenta sprzętu (lub jego przedstawiciela w Polsce) potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta (oświadczenie należy dołączyć do oferty). d) Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera. Oświadczenie producenta sprzętu (lub jego przedstawiciela w Polsce) należy dołączyć do oferty. e) Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001 f) Wymagane okno czasowe dla zgłaszania usterek min wszystkie dni robocze w godzinach od 9:00 do 16:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych – do postępowania należy dostarczyć oświadczenie producenta oferowanego komputera (lub jego przedstawiciela w Polsce) z wyżej wymienionym numerem).
20	System operacyjny	Z uwagi na charakterystykę projektu i fakt, że komputery trafią do rodzin z dziećmi i wykorzystywane będą do nauki zdalnej – zamawiający dopuszcza system operacyjny w wersji edukacyjnej. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.

		12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń

		43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
21	Oprogramowanie dodatkowe	Oprogramowanie dodatkowe pozwalające na: - Szyfrowanie i deszyfrowanie pojedynczych plików i folderów - Zamazywanie plików z dysku twardego zgodne z certyfikatem DoD 5220.22M - Osobisty strzeżony dysk (PSD) w postaci bezpiecznej partycji, w którym można przechowywać poufne pliki. Dostęp do plików zapisanych w formacie PSD można uzyskać tylko po wprowadzeniu uwierzytelniającego hasła. - Ustawienia BIOS: ustawienie sekwencji bootowania, ustawienie haseł dostępu, Import/Export ustawień, blokowanie portów i urządzeń. Do oferty należy dołączyć oświadczenie producenta oferowanego komputera (lub jego przedstawiciela w Polsce), że oferowane oprogramowanie jest w pełni kompatybilne z oferowanym sprzętem. W ofercie należy podać nazwę oferowanego oprogramowania dodatkowego.
22	Certyfikaty i standardy	Certyfikat ISO 9001:2000 dla producenta sprzętu. Certyfikat ISO 14001 dla producenta sprzętu. Deklaracja zgodności CE (załączyć do oferty). Certyfikat potwierdzający spełnianie norm MIL-STD-810G, w zakresie co najmniej: - wysokich oraz niskich temperatur (MIL-STD-810G: 2008, Method 501.5 Procedure I and II oraz MIL-STD-810G: 2008, Method 502.5 Procedure I and II) - deszczu i wilgotności (w tym odporności klawiatury na zalanie) (MIL-STD-810G: 2008, Method 506.5 Procedure III oraz MIL-STD-810G: 2008, Method 507.5 Procedure I) - upadek (MIL-STD-810G: 2008, Method 516.6 Procedure IV) Standard TED – THE ECO Declaration. Certyfikat Energy Efficiency Certification.
23	Wsparcie techniczne producenta	A) Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. B) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. C) W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji. D) Do oferty należy dołączyć kartę katalogową/specyfikację techniczną urządzenia. Karta powinna zawierać wyraźne zdjęcia obudowy oferowanego komputera.
24	Wyposażenie dodatkowe	1. Myszka bezprzewodowa,

25	Pakiet biurowy	
	Pakiet biurowy	Pakiet oprogramowania biurowego zawierającego minimum: 1. arkusz kalkulacyjny, 2. edytor tekstu 3. program do prezentacji Pakiet aplikacji biurowych musi umożliwić prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC, .DOCX, .XLS, .XLSX,, .PPT, .PPTX, w tym obsługa formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013 i MS Office 2016, bez utraty danych oraz bez konieczności reformatowania dokumentów, Edytor tekstów musi umożliwiać: 1. 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.

		2. wstawianie oraz formatowanie tabel. 3. wstawianie oraz formatowanie obiektów graficznych. 4. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. 5. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. 6. automatyczne tworzenie spisów treści. 7. formatowanie nagłówków i stopek stron. 8. śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. 9. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. 10. określenie układu strony (pionowa/pozioma). 11. wydruk dokumentów. 12. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. 13. pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010 i 2013, wykorzystywanych przez Zamawiającego, z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. 14. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 15. wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem. 16. 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. Arkusz kalkulacyjny musi umożliwiać: 1. tworzenie raportów tabelarycznych 2. tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych 3. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. 4. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBGC, pliki tekstowe, pliki XML, webservice) 5. obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. 6. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych 7. wyszukiwanie i zamianę danych 8. wykonywanie analiz danych przy użyciu formatowania warunkowego 9. nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie 10. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności 11. formatowanie czasu, daty i wartości finansowych z polskim formatem 12. zapis wielu arkuszy kalkulacyjnych w jednym pliku. 13. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010 i 2013 wykorzystywanych przez Zamawiającego, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. 14. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: 1. przygotowywanie prezentacji multimedialnych, które będą:

		2. prezentowanie przy użyciu projektora multimedialnego 3. drukowanie w formacie umożliwiającym robienie notatek 4. zapisanie jako prezentacja tylko do odczytu 5. nagrywanie narracji i dołączanie jej do prezentacji 6. opatrywanie slajdów notatkami dla prezentera 7. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo 8. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego 9. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym 10. możliwość tworzenia animacji obiektów i całych slajdów prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera 11. pełna zgodność z formatami plików utworzonych za pomocą oprogramowania Microsoft PowerPoint 2003, 2007, 2010 i 2013 wykorzystywanych przez Zamawiającego. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać: 1. tworzenie i edycję drukowanych materiałów informacyjnych 2. tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów. edycję poszczególnych stron materiałów. 3. podział treści na kolumny. 4. umieszczanie elementów graficznych. 5. wykorzystanie mechanizmu korespondencji seryjnej 6. płynne przesuwanie elementów po całej stronie publikacji. 7. eksport publikacji do formatu PDF oraz TIFF. 8. wydruk publikacji. 9. możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

26	Pakiet antywirusowy	
	Pakiet antywirusowy	**Administracja zdalna** 1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux. 2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD. 3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik. 5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. 6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy. 9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6. 10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs. 11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji. 12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym. 14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.

		15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 17. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image". 18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów. 19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy. 20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS. 23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP. 24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11. 25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. 26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych. 27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów. 28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 29. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 30. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. 31. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS. 32. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci. 33. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 34. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające. 35. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania. 36. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 37. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny. 38. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. 39. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 40. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS. 41. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. 42. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi. 43. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

		44. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 45. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 46. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej. 47. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany. 48. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 50. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych. 51. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 52. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. 53. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. 54. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 55. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 56. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. 57. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. 58. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. 59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej. 60. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. 61. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. 62. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta. 63. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. 64. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. 65. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. 66. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. 67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. 68. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny. 69. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV. 70. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.

		71. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. 72. Powiadomienia mailowe mają być wysyłane w formacie HTML. 73. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. 74. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 75. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 76. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. 77. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami. 78. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. 79. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu. 80. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. 81. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan. 82. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. 83. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. 84. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych. 85. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. 86. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. 87. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. 88. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie. 89. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego. 90. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. 91. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault). 92. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk. 93. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal). 94. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

2. Zaoferowany sprzęt będący przedmiotem zamówienia winien być fabrycznie nowy, nieużywany, nieuszkodzony, nieobciążony prawami osób trzecich.
3. Zamówienie obejmuje transport Wykonawcy oraz wniesienie do pomieszczeń wskazanych przez Zamawiającego,
4. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika oraz karty gwarancji producenta.