Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
System operacyjny	Klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Interfejs graficzny użytkownika pozwalający na obsługę: a. Klasyczną przy pomocy klawiatury i myszy, b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych, 2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim, 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe, 4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje, 5. Wbudowany system pomocy w języku polskim; 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, 7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne, 10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego, 11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, 12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, 14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), 15. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer, 16. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji, 17. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji, 18. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe, 19. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 20. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 21. 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, 22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 23. Obsługa standardu NFC (near field communication), 24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 27. Mechanizmy uwierzytelniania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.

	28. Mechanizmy wieloskładnikowego uwierzytelniania. 29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5, 30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, 31. Wsparcie dla algorytmów Suite B (RFC 4869) 32. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji, 33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku 34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym, 35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny, 36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0, 37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji, 38. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu, 39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec, 40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach, 42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń, 43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem, 44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning) 45. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową, 46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację, 47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, 48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 49. Udostępnianie wbudowanego modemu, 50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej, 51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, 52. 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.), 53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu), 54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych, 55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika, 56. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych 58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 59. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. 60. System o architekturze 64bitowej, nie wymagający aktywacji za pomocą telefonu lub Internetu, instalacja bez potrzeby ręcznego wpisywania klucza, załączony nośnik do komputera. 61. Możliwość, w ramach posiadanej licencji, do używania wcześniejszych wersji oprogramowania systemowego. Dopuszcza się zainstalowanie wcześniejszej wersji systemu z możliwością aktualizacji do wymaganej. System musi zapewniać pełną integrację z wdrożoną usługą katalogową w siedzibie Zamawiającego.

Określenie w OPZ „system operacyjny Microsoft Windows 10 Professional PL" należy odczytywać „Wymagane minimalne parametry techniczne komputerów" – podane w tym pliku.