Parametry równoważności dla systemu operacyjnego:

Opis wymagań minimalnych
Producent, nazwa, wersja
System operacyjny musi spełniać następujące wymagania minimalne 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. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
4. Wbudowany system pomocy w języku polskim;
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
7. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
8. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
9. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
10. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
11. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug & Play, WiFi),
12. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
13. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego;
14. Obsługa standardu NFC (near field communication),
15. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
16. Wsparcie wbudowanej zapory ogniowej dla Internet .
17. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych .
18. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
19. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,

20. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień.
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. 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.
24. Mechanizmy wieloskładnikowego uwierzytelniania.
25. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
26. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
27. Wsparcie dla algorytmów Suite B (RFC 4869)
28. 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.
29. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym.
30. Wsparcie dla środowisk .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
31. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
32. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego.
33. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
34. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).