OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa subskrypcji oprogramowania typu Microsoft 365 for Education A3 ShrdSvr ALNG SubsVL MVL PerUsr dla Uniwersytetu Ekonomicznego we Wrocławiu

Przedmiotem zamówienia jest dostawa subskrypcji oprogramowania typu Microsoft 365 for Education A3 Unified ShrdSvr ALNG SubsVL MVL PerUsr lub równoważnego w ramach rocznej umowy subskrypcyjnej (EES) dla pracowników i studentów Uniwersytetu Ekonomicznego we Wrocławiu

Zamawiający wymaga aby ww. oprogramowanie zawierało co najmniej subskrypcje licencji (AAD-38391): systemu operacyjnego, pakietu biurowego, usługi zarządzania urządzeniami i tożsamością użytkowników, spełniające wymagania określone w niniejszym załączniku,

Liczba subskrypcji 1100 szt.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Interfejs graficzny całości oprogramowania dla 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 obligatoryjnie w języku polskim i języku angielskim.
3. Wbudowany system pomocy w języku polskim.
4. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
5. 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.
6. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizmów zarządzany przez administratora systemu Zamawiającego.
7. Wbudowana zapora Internetowa (firewall) dla ochrony połączeń internetowych.
8. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
9. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
10. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
11. Możliwość zarządzania stacją roboczą poprzez polityki grupowe - przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji i dla wskazanych aplikacji.
12. Rozbudowane, definiowalne polityki bezpieczeństwa - polityki dla systemu operacyjnego.
13. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.

16. 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.
17. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); Wsparcie dla IPSEC oparte na politykach - wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
18. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 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.
19. Mechanizmy wieloskładnikowego uwierzytelniania. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5, Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu, Wsparcie dla algorytmów Suite B (RFC 4869).
20. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji.
21. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny, (OMA) Device Management (DM) protocol 2.0.
22. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji.
23. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu.
24. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
25. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
26. Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
27. Wsparcie dla JScript i VBScript - możliwość uruchamiania interpretera poleceń.
28. Zdalna pomoc i współdzielenie aplikacji - możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
29. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego (provisioning).
30. 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.
31. Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
32. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla

użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe, Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.

33. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
34. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
35. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
36. 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.
37. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
38. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
39. Możliwość Instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
40. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
41. Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTIP i SMB.
42. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tych polityk.
43. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC.
44. Mechanizm umożliwiający naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
45. Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient- serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji.
46. Pakiet biurowy musi być w pełni kompatybilny (bez konieczności dodatkowego instalowania i używania konwerterów, edytorów, nakładek, itd.) z posiadaną przez Zamawiającego usługą MS Office 365 on-line.
47. Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia

dodatkowych aplikacji:

a) dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie właściwe ponad 2GB przestrzeni adresowej.

48. Wymagania odnośnie interfejsu użytkownika:
    a) pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
    b) możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
49. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
50. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych. musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
    a) posiada kompletny i publicznie dostępny opis formatu,
    b) ma zdefiniowany układ informacji w postaci XML zgodnie z aktualnymi przepisami prawa w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
    c) umożliwia kreowanie plików w formacie XML.
51. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
52. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
53. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
54. 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 tworzenia i pracy z lokalną bazą danych,
    f) narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
    g) narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR,
    h) narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
55. Subskrypcja pakietu usług zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:
    a) pakiet aplikacji biurowych dostępny w wersji instalowanej klasycznych aplikacji dostępny dla pięciu urządzeń pojedynczego użytkownika (5 komputerów PC oraz 5 urządzeń mobilnych),
    b) poczta e-mail ze skrzynką pocztową o pojemności min. 100 GB,
    c) nieograniczony osobisty magazyn w chmurze,
    d) zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,

e) zagwarantowanie poziomu dostępności usługi (SLA) na poziomie 99,9% w skali roku (lub wyższym),
f) stałe modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, zgodne ze standardami ISO 27017 i 27018,
g) dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO 27017 i 27018,
h) możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,
i) możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
j) dostępność mechanizmów monitorowania zachowania użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych,
k) możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej,
l) możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory,
m) dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione",
n) dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
o) możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
p) mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.

56. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
57. Gwarancja braku dostępu do danych Zamawiającego, przetwarzanych w ramach pakietu usług, z wyłączeniem działań serwisowych wymagających każdorazowo zgody Zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.
58. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur).
59. Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
    a) integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy,
    b) wykorzystanie bazy użytkowników znajdujących się w Active Directory,
    c) inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
    d) inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji: nazwa urządzenia, identyfikator urządzenia, nazwa platformy systemu operacyjnego, wersja oprogramowania układowego, typ procesora, model urządzenia, producent urządzenia, lista aplikacji zainstalowanych w ramach przedsiębiorstwa.
60. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych.
61. Usługa ma umożliwiać dystrybucji oprogramowania na żądanie użytkownika, realizowane poprzez

wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji.

62. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
63. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji.
64. System i pakiet aplikacji musi być w pełni kompatybilny z wdrożonymi i użytkowanymi przez Zamawiającego aplikacjami zainstalowanymi i użytkowanymi na współpracujących zasobach: Simple ERP, USOS, Płatnik ZUS. W przypadku zaoferowania systemu równoważnego oferent winien skonfigurować każdy z komputerów do pracy z wszystkimi wyżej wymienionymi programami oraz w okresie gwarancji zapewnić wsparcie przy konfiguracji w przypadku aktualizacji wszystkich wyżej wymienionych programów.
65. System musi umożliwiać hosting spotkań dla ok. 10000 osób dla aplikacji Skype.
66. System planowania spotkań z wykładowcami przy użyciu usługi MS Booking lub równoważnej z jej wszystkimi właściwościami.
67. Udostępnienie w subskrypcji Profesjonalnych Grup Learningowych.