|  |
| --- |
| **ZAŁĄCZNIK NR 3** |

**Wykonawca:**

………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia jest dostawa subskrypcji pakietu Office 365 dla 200 użytkowników na  okres 12 miesięcy w ramach licencjonowania grupowego Microsoft MPSA, uprawniających Uniwersytet Przyrodniczy w  Poznaniu do instalacji na posiadanych komputerach PC z systemem operacyjnym Windows 11, Windows 10 oraz Mac OS i  użytkowania poniższego oprogramowania.
2. Zamawiający odrzuci ofertę, której parametry nie będą spełniały wymagań opisu przedmiotu zamówienia.
3. Zamawiający wymaga aby dostarczone rozwiązanie było w wersji aktualnej lub opisanej przez Zamawiającego tj. najnowszej, stabilnej, opublikowanej przez producenta, zapewniającej zgodność i wymaganą funkcjonalność.
4. Dostawa nastąpi w sposób elektroniczny, bez udziału fizycznych nośników, za  pośrednictwem portalu licencjonowania zbiorowego Microsoft, z którego możliwe jest  pobieranie plików instalacyjnych oraz kluczy instalacyjnych oprogramowania. W  przypadku produktów równoważnych udostępniony zostanie portal umożliwiający pobranie zamawianych produktów.

|  |
| --- |
| Przedmiotem zamówienia jest pakiet Microsoft Office 365 E3 dla 200 użytkowników na okres 12 miesięcy lub produkt równoważny (licencja subskrypcyjna na użytkownika) |
| Pakiet subskrypcji usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego musi zawierać następujące oprogramowanie i usługi:  **System operacyjny klasy desktop.**  System operacyjny klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Interfejs graficzny użytkownika pozwalający na obsługę: 2. klasyczną przy pomocy klawiatury i myszy 3. dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 4. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym polskim i  angielskim 5. Zlokalizowane w języku polskim, co najmniej następujące elementy menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe. 6. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje. 7. Wbudowany system pomocy w języku polskim. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 9. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 10. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z  modułem „uczenia się” głosu użytkownika. 11. 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. 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 13. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 14. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z  systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 15. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z  zapewnionymi bezpłatnymi aktualizacjami. 16. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 17. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 18. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i  dla  wskazanych aplikacji. 19. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 20. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 21. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 22. 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. 23. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 24. Obsługa standardu NFC (near field communication). 25. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 26. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 27. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 28. Mechanizmy uwierzytelniania w oparciu o: 29. Login i hasło, 30. Karty z certyfikatami (smartcard), 31. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 32. 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 zgodny ze specyfikacją FIDO. 33. Mechanizmy wieloskładnikowego uwierzytelniania. 34. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 35. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 36. Wsparcie dla algorytmów Suite B (RFC 4869). 37. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji. 38. 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. 39. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym. 40. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny. 41. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0. 42. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji. 43. Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu. 44. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 45. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i  ich  odtwarzania oraz generowania raportów z ustawień polityk. 46. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 47. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 48. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 49. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego (provisioning). 50. 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. 51. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 52. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla  użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 53. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 54. Udostępnianie wbudowanego modemu. 55. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 56. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 57. 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.). 58. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 59. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 60. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 61. 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. 62. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych 63. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 64. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. 65. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB), 66. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z  mechanizmem wyszukiwania danych w systemie 67. 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. 68. 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 wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB. 69. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk. 70. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od  przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC. 71. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami. 72. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC. 73. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów. 74. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M. 75. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w  momencie braku możliwości jego uruchomienia. 76. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w  momencie braku możliwości jego uruchomienia. 77. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”. 78. 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. 79. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością. 80. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji. 81. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej. 82. Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub  przebudowywania paczek aplikacji. 83. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji. 84. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika. 85. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym. 86. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB. 87. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet. 88. Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.   **Subskrypcja usługi hostowanej i pakietu biurowego.**  Subskrypcja powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of- The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi katalogowej typu LDAP, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Ponadto musi zawierać subskrypcję pakietu biurowego.  Wymagania dotyczące usługi hostowanej:   1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę katalogową. 2. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla  użytkowników logujących się do własnej usługi katalogowej Active Directory. 3. Możliwość dodawania własnych nazw domenowych do usługi katalogowej. 4. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup. 5. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z  poczty elektronicznej i przechowywanych plików. 6. W okresie obowiązywania subskrypcji Usługa będzie przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, w przypadku podjęcia decyzji o baraku jej kontynuacji, Usługa będzie przechowywać dane Zamawiającego, które zostały w niej zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po  upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją Usługi zostanie wyłączone a dane Zamawiającego zostaną usunięte. 7. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS. 8. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich. 9. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego. 10. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego. 11. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego. 12. Usługa musi odpowiadać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych. 13. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych. 14. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.   **Usługa poczty elektronicznej on-line**   1. Usługa musi umożliwiać:    1. obsługę poczty elektronicznej,    2. zarządzanie czasem,    3. zarządzania zasobami,    4. zarządzanie kontaktami i komunikacją. 2. Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:    1. zarządzania użytkownikami poczty,    2. wsparcia migracji z innych systemów poczty,    3. wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,    4. wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty,    5. dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:       * posiadanego oprogramowania Outlook (2013, 2016, 2019, 2021),       * przeglądarki (Web Access),       * urządzeń mobilnych. 3. Wymagane cechy usługi to: 4. skrzynki pocztowe dla każdego użytkownika o pojemności minimum 40 GB, 5. standardowy i łatwy sposób obsługi poczty elektronicznej, 6. obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari, 7. współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy, 8. bezpieczny dostęp z każdego miejsca, w którym jest dostępny Internet. 9. Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:    1. Funkcjonalność podstawowa:  * odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych, * mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata, * tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami, * zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia, * wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.   1. Funkcjonalność wspierająca pracę grupową: * Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy  do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości. * Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu. * Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze. * Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone. * Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania. * Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań. * Obsługa list i grup dystrybucyjnych. * Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów. * Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu. * Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności. * Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami. * Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności. * Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego. * Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów. * Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków. |

**Równoważność produktów:**

Dopuszcza się możliwość zaoferowania produktów równoważnych, zgodnie z opisem poniżej.

Zamawiający wymaga, aby oferowane produkty równoważne spełniały wymagania określone w  powyższej tabeli oraz niżej wymienione wymagania.

1. Produkt równoważny musi bez zakłóceń współpracować z posiadaną przez Zamawiającego infrastrukturą sprzętową oraz wykorzystywanym oprogramowaniem i systemami, do których należą: serwery, laptopy, komputery stacjonarne, urządzenia drukujące i skanujące, urządzenia sieciowe, oprogramowanie systemowe Microsoft Windows, Windows Server, oprogramowanie Microsoft SharePoint i Project Server, środowisko wirtualizacyjne VmWare, aplikacje do obsługi GMG. Na Wykonawcy oferującym produkty równoważne spoczywa odpowiedzialność w zakresie prawidłowego działania zaoferowanych produktów w środowisku pracy użytkowników produktów po stronie Zamawiającego.
2. Wykonawca musi zapewnić warunki i zakres usługi wsparcia technicznego producenta dla  produktów równoważnych nie gorsze niż usługa określona dla odpowiedniego produktu producenta Microsoft.
3. Wykonawca musi wykazać, że funkcjonalność każdego produktu równoważnego nie jest gorsza od funkcjonalności odpowiedniego produktu producenta Microsoft.
4. Wykonawca musi zapewnić, że produkty równoważne są kompatybilne i będą w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem systemowym, aplikacyjnym i  użytkowym, eksploatowanym i obsługiwanym przez Zamawiającego.
5. Wykonawca zobowiązany jest przeszkolić pracowników Zamawiającego w zakresie funkcjonalności i działania produktów równoważnych w terminie ustalonym z Zamawiającym, lecz nie później niż w okresie 30 dni kalendarzowych od daty zawarcia Umowy.
6. Wykonawca zobowiązany jest pokryć koszty zmiany w zakresie produktów Microsoft na produkty i rozwiązania równoważne, konieczne do właściwego działania środowiska sprzętowo- programowego Zamawiającego oraz przeszkolenia personelu Zamawiającego, o ile wystąpi taka konieczność;
7. Wykonawca zobowiązany jest przywrócić sprawne działanie infrastruktury sprzętowo- programowej Zamawiającego na własny koszt dokonać niezbędnych modyfikacji przywracających właściwe działanie tego środowiska sprzętowo-programowego, również po odinstalowaniu produktu równoważnego w przypadku, gdy zaoferowane produkty równoważne nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym lub spowoduje zakłócenia w funkcjonowaniu pracy tego środowiska sprzętowo-programowego.

…………………dnia ……………