Zakup sfinansowany w ramach realizacji projektu „Cyfrowa Gmina” finansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020.

Opis kryteriów równoważnych.

Jeżeli Zamawiający określił w OPZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

I. Zamawiający dopuszcza zaoferowanie produktów równoważnych do oprogramowania Microsoft Office Home & Business 2021 PL

1. W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w OPZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w OPZ, w szczególności w zakresie:
    1) warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania Microsoft Office Home & Business 2021 PL,
    2) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w punkcie III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego”,
    3) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Microsoft Windows 10 Professional/Enterprise, Microsoft Exchange, Microsoft ADDS, MAC OS funkcjonującym u Zamawiającego,
    4) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,

5) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
6) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem Microsoft Windows 10 Professional/Enterprise i Microsoft Exchange 2013/2016.

2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.
4. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.

II. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Przeprowadzić autoryzowane warsztaty dla administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiających pełne poznanie produktu równoważnego, Wykonawca w terminie 5 dni od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram warsztatów, Wykonawca w ramach warsztatów zapewni salę szkoleniową. Czas trwania każdego z warsztatów nie może być krótszy niż 5 (pięć) dni roboczych w następujących po sobie dniach roboczych.
2. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym Zamawiającego w terminie do 5 dni roboczych od dnia zakończenia warsztatów z pkt II. 1.
3. Dostarczyć wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego

1. <u>Funkcjonalność oprogramowania równoważnego do systemu operacyjnego Windows 10 Professional/Enterprise:</u>
    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 równoważnym systemem operacyjnym 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 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) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
50) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
51) 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.).
52) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

53) Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
54) Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
55) Wbudowane w równoważnym systemie operacyjnym 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.
56) Wbudowane w równoważny system operacyjny narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
57) Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
58) Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
59) Mechanizm instalacji i uruchamiania równoważnego systemu operacyjnego
z pamięci zewnętrznej (USB).
60) 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.
61) 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.

62) Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
63) Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom,

    w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC.
64) Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
65) Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
66) Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów.
67) Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M.
68) Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
69) Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia.
70) Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”.
71) 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.

72) Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością.
73) Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji.
74) Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
75) Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
76) Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
77) Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
78) Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
79) Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
80) Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
81) Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.

2. <u>Funkcjonalność oprogramowania równoważnego do pakietu biurowego Microsoft Office 365:</u>

   Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

   1) Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.

2) 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. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
    c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu system operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3) Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
4) Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5) Oprogramowanie 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 Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526).
    c. Umożliwia kreowanie plików w formacie XML.
    d. Wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES.
6) Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.

7) Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami
   i aplikacjami (język makropoleceń, język skryptowy).
9) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10) 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.
11) Edytor tekstów musi umożliwiać.
    a. 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.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.

e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
g. Automatyczne tworzenie spisów treści.
h. Formatowanie nagłówków i stopek stron.
i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
l. Określenie układu strony (pionowa/pozioma).
m. Wydruk dokumentów.
n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007, Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
p. Zapis i edycję plików w formacie PDF.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco.
s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.

12) Arkusz kalkulacyjny musi umożliwiać:
a. Tworzenie raportów tabelarycznych.
b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.

c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
g. Wyszukiwanie i zamianę danych.
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
i. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS.
j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
l. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz

Microsoft Excel 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.

q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

13) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
    a. Przygotowywanie prezentacji multimedialnych, które będą:
        - Prezentowane przy użyciu projektora multimedialnego.
        - Drukowane w formacie umożliwiającym robienie notatek.
    b. Zapisanie jako prezentacja tylko do odczytu.
    c. Nagrywanie narracji i dołączanie jej do prezentacji.
    d. Opatrywanie slajdów notatkami dla prezentera.
    e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
    f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
    g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
    h. Możliwość tworzenia animacji obiektów i całych slajdów.
    i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
    j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010 i 2013.
14) Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
    a. Tworzenie i edycję drukowanych materiałów informacyjnych.
    b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
    c. Edycję poszczególnych stron materiałów.
    d. Podział treści na kolumny.

e. Umieszczanie elementów graficznych.
f. Wykorzystanie mechanizmu korespondencji seryjnej.
g. Płynne przesuwanie elementów po całej stronie publikacji.
h. Eksport publikacji do formatu PDF oraz TIFF.
i. Wydruk publikacji.
j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

15) Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
    a. Tworzenie bazy danych przez zdefiniowanie:
    b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
    c. Relacji pomiędzy tabelami.
    d. Formularzy do wprowadzania i edycji danych.
    e. Raportów.
    f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych.
    g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów.
    h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
16) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
    a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory.
    b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
    c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
    d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
    e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
    f. Automatyczne grupowanie poczty o tym samym tytule.

g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
j. Zarządzanie kalendarzem.
k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
l. Przeglądanie kalendarza innych użytkowników.
m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
n. Zarządzanie listą zadań.
o. Zlecanie zadań innym użytkownikom.
p. Zarządzanie listą kontaktów.
q. Udostępnianie listy kontaktów innym użytkownikom.
r. Przeglądanie listy kontaktów innych użytkowników.
s. Możliwość przesyłania kontaktów innym użytkowników.
t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

17) Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
a. Pełna polska wersja językowa interfejsu użytkownika.
b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX 10 lub wyższych.
d. 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.

e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
g. Obsługa telekonferencji SKW:
    - Dołączania do telekonferencji.
    - Szczegółowej listy uczestników.
    - Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    - Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    - Głosowania.
    - Udostępniania plików i pulpitów.
    - Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji.
h. Możliwość zmiany kanału komunikacji z pośrednictwem wiadomości błyskawicznych do połączenia głosowego i/lub wideo w ramach pojedynczej, otwartej w aplikacji sesji (bez konieczności przełączania się pomiędzy aplikacjami).
i. Lista adresowa wraz ze statusem obecności, opisem użytkowników SKW, zdjęciami użytkowników, listą dostępnych do komunikacji z nimi kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji oraz wydzielania grup kontaktów typu ulubione lub ostatnie.
j. Status obecności, dający możliwość ręcznego ustawiania statusu (dostępny, zajęty, nie przeszkadzać, z dala od komputera, niedostępny), automatycznej synchronizacji z jego aktywnością w systemie operacyjnym stacji roboczej, a w przypadku instalacji wybranych systemów poczty elektronicznej – dostępu do

informacji o dostępności użytkownika na bazie wpisów do jego kalendarza.

k. Możliwość rozszerzania listy adresowej o zewnętrznych użytkowników wraz z informacjami opisowymi i kontaktowymi.
l. Historia ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień.
m. Integracja ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
n. Definiowanie i konfiguracja urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

3. <u>Funkcjonalność oprogramowania równoważnego do portalu on-line do zażądania użytkownikami, licencjami.</u>

   Portal on-line musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

   1) Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych.
   2) Zarządzanie strukturą portalu i treściami www.
   3) Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści.
   4) Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej.
   5) Tworzenie repozytoriów wzorów dokumentów.
   6) Tworzenie repozytoriów dokumentów.

7) Wspólną, bezpieczną pracę nad dokumentami.
8) Wersjonowanie dokumentów (dla wersji roboczych).
9) Organizację pracy grupowej.
10) Wyszukiwanie treści.
11) Dostęp do danych w relacyjnych bazach danych.
12) Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13) Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów. Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio jako wbudowane właściwości produktu:
    a. Interfejs użytkownika:
        - Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
        - Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0.
        - Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów.
        - Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego.
        - Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej

dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).

b. Projektowanie stron
    - Wbudowane intuicyjne narzędzia projektowania wyglądu stron.
    - Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML.
    - Wsparcie dla ASP.NET, Apache, C#, Java i PHP.
    - Możliwość osadzania elementów iFrame w polach HTML na stronie.
c. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
    - Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili.
    - Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów.
    - Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili.
    - Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego.
    - Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services.

- Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

Oprogramowanie portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę.

4. <u>Funkcjonalność oprogramowania równoważnego do pakietu biurowego on-line dostępnego przez przeglądarkę.</u>

   Pakiet biurowy on-line musi spełniać następujące wymagania:

   1) Wymagania odnośnie interfejsu użytkownika:
      a. Pełna polska wersja językowa interfejsu użytkownika.
      b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   2) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
      a. posiada kompletny i publicznie dostępny opis formatu.
      b. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766).
   3) Pakiet biurowy on-line musi zawierać:
      a. Edytor tekstów.
      b. Arkusz kalkulacyjny.
      c. Narzędzie do przygotowywania i prowadzenia prezentacji.
      d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
      e. Musi być w pełni kompatybilny z posiadanym przez Zamawiającego oprogramowaniem pakietów biurowych – MS Office 2010, MS Office 2013, MS Office 2016, MS Exchange 2013, MS Visio 2013, MS Project 2013

4) Edytor tekstów musi umożliwiać:
    a. 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.
    b. Wstawianie oraz formatowanie tabel.
    c. Wstawianie oraz formatowanie obiektów graficznych.
    d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    f. Automatyczne tworzenie spisów treści.
    g. Formatowanie nagłówków i stopek stron.
    h. Sprawdzanie pisowni w języku polskim.
    i. Śledzenie zmian wprowadzonych przez użytkowników.
    j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    k. Określenie układu strony (pionowa/pozioma).
    l. Wydruk dokumentów.
    m. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    n. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    o. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
    p. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu

umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.

q. 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.

5) Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych.
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).
   e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
   f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
   g. Wyszukiwanie i zamianę danych.
   h. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
   i. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
   j. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   k. Formatowanie czasu, daty i wartości finansowych z polskim formatem.

l. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

6) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
   a. Przygotowywanie prezentacji multimedialnych, które będą:
      - Prezentowane przy użyciu projektora multimedialnego.
      - Drukowane w formacie umożliwiającym robienie notatek.
      - Zapisane jako prezentacja tylko do odczytu.
      - Nagrywane narracji i dołączanie jej do prezentacji.
      - Opatrywane notatkami dla prezentera.
   b. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
   c. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
   d. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
   e. Możliwość tworzenia animacji obiektów i całych slajdów.
   f. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
   g. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, 2010 i 2013.

5. <u>Funkcjonalność oprogramowania równoważnego do serwera komunikacji wielokanałowej online (SKW).</u>

   Funkcjonalność wspomagająca wewnętrzną i zewnętrzną komunikację ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1) Bezpieczną komunikację głosową oraz video.
2) Przesyłanie wiadomości błyskawicznych (tekstowych).
3) Możliwość organizowania telekonferencji.
4) Możliwość współdzielenia dokumentów w trakcie spotkań on-line (zdalnych).

6. Funkcjonalność oprogramowania równoważnego do repozytorium dokumentów.

   Repozytorium dokumentów musi zapewnić przestrzeń dyskowej o pojemności minimum 1 TB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na:

   1) traktowanie go, jako własnego dysku.
   2) synchronizację zawartości wybranego folderu ze stacji roboczej do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia.
   3) synchronizację zawartości repozytorium z wieloma urządzeniami w ramach uprawnień użytkownika - właściciela repozytorium.

7. Funkcjonalność oprogramowania do zarządzania urządzeniami oraz tożsamością użytkowników.

   Powyższa funkcjonalność musi spełniać następujące wymagania:

   1) Pełne zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT).
   2) Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych.
   3) Portal klasy self-serivce dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej.
   4) Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS).
   5) Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

1) Wykorzystanie telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS podczas dostępu do aplikacji webowych pozwala na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia.
2) Możliwość wydajnej pracy przez użytkowników na licznych lubianych przez nich narzędziach, zapewnia im dostęp do potrzebnych aplikacji.
3) Jednokrotne logowanie w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika ułatwia pracę użytkownika i redukuje przestoje czasowe.
4) Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwala na redukcję ilości zgłoszeń działów wsparcia nawet o 30%.
5) Automatyczne przepływy pracy i reguł biznesowych pozwalają na zaoszczędzenie czasu 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 reguł biznesowych).
6) Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwala na audyt i kontrolę zgodności z przepisami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
7) Zarządzanie urządzeniami mobilnymi pozwala na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwia zdalne kasowanie danych firmowych lub całego urządzenia.

Dodatkowo funkcjonalność musi składać się z poniższych podsystemów:

1. Podsystem zarządzania tożsamością.
2. Podsystem zarządzania urządzeniami mobilnymi.
3. Podsystem ochrony informacji.
4. Podsystem usługi katalogowej.

1. Podsystem zarządzania tożsamością:

   System zarządzania tożsamością elektroniczną ma zapewniać agregację oraz synchronizacje danych o użytkownikach różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego Centrum certyfikacji.

   Wymagania ogólne:

   1) Bezpieczeństwo:

      System zarządzania tożsamością musi umożliwiać zastosowanie przy połączeniu ze źródłami danych mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji). System powinien zapewniać również prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej poprzez zapory firewall oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).

   2) System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

   3) Skalowalność:

      System zarządzania tożsamością dostarczony w ramach zamówienia musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie od 2 500 do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.

   4) Interoperacyjność:

      System zarządzania tożsamością powinien zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem. System zarządzania tożsamością powinien zapewniać możliwość

realizacji dwukierunkowej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

5) Rozszerzalność:

   System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości funkcjonalności o połączenia z innymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu. System zarządzania tożsamością powinien umożliwiać rozszerzenie w przyszłości rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.

2. <u>Podsystem zarządzania urządzeniami mobilnymi.</u>

   Dostępna poprzez Internet na zasadzie licencji narzędzia pozwalające na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:

   1) Integrację z systemem SCCM 2012 R2 w oparciu o natywne interfejsy komunikacyjne.
   2) Wykorzystanie bazy użytkowników znajdujących się w Active Directory.
   3) Porozumiewania się z użytkownikiem końcowym w języku polskim.

   1) Inwentaryzacja sprzętu i zarządzanie zasobami:
      a. Inwentaryzacja zasobów urządzenia mobilnego odbywa się w interwałach czasowych.
      b. Inwentaryzacja sprzętu pozwala na zbieranie następujących informacji.
         - Nazwa urządzenia.
         - Identyfikator urządzenia.
         - Nazwa platformy systemu operacyjnego.
         - Wersja oprogramowania układowego.
         - Typ procesora.

- Model urządzenia.
- Producent urządzenia.
- Architektura procesora.
- Język urządzenia.
- Lista aplikacji zainstalowanych w ramach przedsiębiorstwa.

2) Zdalna blokada i wymazanie:
    a. W celu zapewnienia bezpieczeństwa danych oprogramowanie musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji.
    b. Oprogramowanie te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
3) Dystrybucja oprogramowania:
    a. Pakiety instalacyjne dla aplikacji mobilnych mogą być przechowywane na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
    b. Systemu UDM umożliwia dystrybucję oprogramowania na prośbę użytkownika, realizowaną poprzez wybór oprogramowania w ramach dostępnego katalogu aplikacji.
    c. Katalog aplikacji jest zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
    d. Katalog aplikacji wspiera następujące formaty aplikacji mobilnych:

- *.appx (Windows RT),
- *.xap (Windows Phone 8),
- *.ipa (iOS),
- *.apk (Android).

e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
   - Windows Store.
   - Windows Phone Store.
   - Android Google Play Store.
   - iOS App Store.

4) Definiowanie polityk urządzenia mobilnego:
   a. Komponenty umożliwiające zdefiniowanie standardu polityk urządzenia mobilnego.

      W obszarze polityki haseł system zapewni:
      - Zdefiniowanie wymuszenia hasła.
      - Określenia minimalnej długości hasła.
      - Określenia czasu wygasania hasła.
      - Określenia ilości pamiętanych haseł.
      - Określenia ilości prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia.
      - Określenia czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła.

5) Raportowanie, prezentacja danych:

   Oprogramowanie ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika.

3. Podsystem ochrony informacji

   Oprogramowanie bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem.

   Oprogramowanie musi spełniać następujące wymagania:

   1) Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), a nie fizyczne miejsce jej przechowywania.
   2) Oprogramowanie musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs.
   3) Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji.
   4) Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji.
   5) Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, np.:
      a. Brak uprawnień dostępu do informacji.
      b. Informacja tylko do odczytu.
      c. Prawo do edycji informacji.
      d. Brak możliwości wykonania systemowego zrzutu ekranu.
      e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej.
      f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej.
      g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
   6) Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej.

7) Możliwość wyboru restrykcji dostępu w postaci standardowych, łatwych do wyboru szablonów, powstałych na bazie polityk ochrony informacji.
8) Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji.
9) Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT.
10) Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

4. Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

1) Możliwość zintegrowania jednokrotnego logowania (SSO) dla ponad 2500 popularnych aplikacji typu SaaS.
2) Możliwość publikacji aplikacji webowych z wewnątrz organizacji.
3) Możliwość połączenia z usługą Active Directory wewnątrz organizacji.
4) Konsolę zarządzania tożsamością i dostępem.
5) Scentralizowane zarządzanie przydzielania dostępu do aplikacji.
6) Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych).
7) Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP).
8) Samoobsługowe resetowania hasła.
9) Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników.