

I. PRZEDMIOT ZAMÓWIENIA

Zakup licencji na oprogramowanie oraz jego uaktualnienia w ramach umowy licencyjnej na użytkowanie wyspecyfikowanego oprogramowania oraz usług

Wspólny Słownik Zamówień (CPV):

48517000-5 Pakiety oprogramowania informatycznego
 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
 48500000-3 Pakiety oprogramowania komunikacyjnego i multimedialnego
 48620000-0 Systemy operacyjne
 72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia
 72212311-2 Usługi opracowywania oprogramowania do zarządzania dokumentami
 72212610-8 Usługi opracowywania oprogramowania dla baz danych
 72267000-4 Usługi w zakresie konserwacji i napraw oprogramowania
 72263000-6 Usługi wdrażania oprogramowania
 72220000-3 Usługi doradcze w zakresie systemów i doradztwo techniczne
 72250000-2 Usługi w zakresie konserwacji i wsparcia systemów
 80500000-9 Usługi szkoleniowe

1. Specyfikacja ilościowa przedmiotu Zamówienia

Typ oprogramowania	Liczba licencji
Uaktualnienie posiadanych systemów operacyjnych klasy desktop PC	1100
Pakiet biurowy	1100
Pakiet licencji dostępowych	1400
Serwerowy system operacyjny	23
Oprogramowanie do zarządzania środowiskami serwerowymi	23
Serwer poczty elektronicznej typ I	2
Serwer poczty elektronicznej typ II	2
Serwer komunikacji wielokanałowej	1
Serwer zapory ogniowej	1
Serwer wewnętrznego portalu wielofunkcyjnego	1
Serwer wielofunkcyjnego portalu internetowego	2
Serwer relacyjnej bazy danych	2
Serwer zarządzania projektami	1
Pakiet zarządzania projektami	70
Licencje dostępne do serwera zarządzania projektami	100
Zintegrowane środowisko programistyczne	1
Pakiet usług wsparcia technicznego	1
Usługi stowarzyszone	1

Tabela 1 – specyfikacja ilościowa zamawianych produktów

2. Wymagania ogólne

Przedmiotem Zamówienia jest zakup oprogramowania wraz z bezterminowymi licencjami oraz jego aktualizacje w ramach umowy licencyjnej na użytkowanie wyspecyfikowanego oprogramowania,

wraz z prawem do uaktualnienia objętego umową oprogramowania do wersji najbardziej aktualnej w trakcie trwania umowy.

Wymagania ogólne w zakresie licencji:

1. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi (np. w przypadku wymiany stacji roboczej) i zawierać 36 miesięczną usługę uaktualniania wersji zainstalowanego oprogramowania będącego przedmiotem Zamówienia.
2. Licencjonowanie musi uwzględniać prawo do uaktualniania wersji zamawianych produktów w okresie obowiązywania umowy do najnowszych wersji dostępnych na rynku oraz prawa (w okresie przynajmniej 5 lat) instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych.
3. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej licencje pochodzące od jednego producenta, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.
4. W związku z możliwością zwiększenia liczby użytkowników systemów w drugim i trzecim roku trwania Umowy, Zamawiający wymaga zaoferowania licencjonowania umożliwiającego w okresie trwania umowy instalację dodatkowych licencji z zamawianego zakresu produktów z rozliczaniem się za nie post factum - raz do roku.
5. W ramach umowy Zamawiający ma mieć prawo do testowania oprogramowania i korzystania z oprogramowania w celach edukacyjnych wszystkich produktów producenta oprogramowania bez dodatkowych opłat. Wówczas Zamawiający nabywa prawo do uruchamiania:
 - 1.1. 20 kopii każdego produktu w celach edukacyjnych. Na te programy nie trzeba kupować licencji.
 - 1.2. 10 kopii każdego produktu w celach testowych w 60-dniowym okresie ewaluacyjnym, po którym istnieje możliwość Zamówienia odpowiedniej ilości licencji na testowany produkt.
6. Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych (możliwość kopiowania oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.
7. W zakresie wszystkich wymienionych klas oprogramowania Zamawiający wymaga dostarczenia:
 - 7.1. 1 kompletu nośników instalacyjnych uaktualnienia systemów operacyjnych klasy PC i pakietu biurowego umożliwiających instalacje masowe, tzn. instalacje z jednego obrazu systemu.
 - 7.2. Bezterminowych licencji na użytkowanie zamawianego oprogramowania dla produktów, przy których postawił wymaganie dostawy licencji (Tabela 1).
 - 7.3. Kompletu wymaganych kluczy aktywacyjnych.
 - 7.4. Zbiorczych dokumentów pozwalających na stwierdzenie legalności zakupionego oprogramowania dla celów inwentaryzacyjnych i audytowych.

3.Specyfikacja techniczno – eksploatacyjna i cech użytkowych przedmiotu Zamówienia.

W poniższej części przedstawione są wymagania funkcjonalne dotyczące zamawianego oprogramowania i usług.

Z uwagi na to, że art. 30 ust. 5 ustawy prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę jako tego, kto jest zobowiązany wykazać, że oferowane rozwiązania i produkty spełniają wymagania postawione przez Zamawiającego, Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenie pełnej zgodności oferowanych produktów z wymogami specyfikacji.

1.1.Uaktualnienie posiadanych systemów operacyjnych klasy desktop PC

Wymagane jest dostarczenie licencji i nośników umożliwiających instalację systemów operacyjnych na komputerach PC w wersjach 32 i 64 bitowych, jako uaktualnienia systemów zainstalowanych na stacjach roboczych. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;
4. Internetowa aktualizacja zapewniona w języku polskim;
5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe;
7. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);
8. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;
9. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;
10. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;
12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
13. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;
14. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego;
15. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;
16. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;
17. Wbudowany system pomocy w języku polskim;
18. Możliwość przystosowania systemu stacji roboczej dla osób niepełnosprawnych (np. słabo widzących);
19. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
20. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;

21. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
22. Wsparcie dla logowania przy pomocy smartcard;
23. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;
24. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
25. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
26. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
27. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
28. 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;
29. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;
30. Graficzne środowisko instalacji i konfiguracji;
31. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
32. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;
33. Udostępnianie modemu;
34. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
35. Możliwość przywracania plików systemowych;
36. System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);
37. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
38. 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;
39. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych;
40. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych;
41. Możliwość nieodpłatnego instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu;
42. 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;
43. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie;
44. 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;
45. 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;
46. Funkcjonalność umożliwiająca inwentaryzację oprogramowania na stacjach roboczych poprzez sieć Internet - bez konieczności instalacji dodatkowego serwera lub dedykowanego tej funkcjonalności oprogramowania na serwerze wewnątrz infrastruktury informatycznej przedsiębiorstwa;
 47. Mechanizm centralnego zbierania informacji o występujących błędach aplikacji, bez konieczności instalacji oprogramowania typu agent na stacjach roboczych użytkowników;
 48. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk;
 49. Funkcjonalność umożliwiająca kontrolę działań użytkowników w ramach polityk zarządzania komputerami PC;
 50. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC;
 51. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami;
 52. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC;
 53. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów;
 54. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M;
 55. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia;
 56. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia;
 57. Mechanizm przesyłania aplikacji w paczkach, bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”;
 58. 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;
 59. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością;
 60. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji;
 61. Funkcjonalność pozwalająca na zaktualizowanie systemów w czasie pracy użytkowników końcowych na aplikacji tym systemie bez przerywania pracy;
 62. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej;
 63. Funkcjonalność umożliwiająca na zaktualizowanie klienta systemu bez potrzeby aktualizacji, przebudowywania paczek systemu;
 64. Funkcjonalność pozwalająca w swobodny sposób łączyć paczki aplikacji w celu uzyskania dodatkowych funkcjonalności;
 65. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika;
 66. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym;
 67. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB;
 68. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet;

69. Mechanizm umożliwiający uruchomienie starszych wersji systemów operacyjnych na nowym lub tym samym systemie operacyjnym poprzez dostarczenie obrazu wirtualnego systemu operacyjnego poprzez sieć LAN lub WAN;
70. Mechanizm umożliwiający dostarczanie i kontrolę wewnątrz wirtualnego systemu operacyjnego aplikacji niekompatybilnych z nowym systemem operacyjnym;
71. Funkcjonalność pakowania (zmniejszania wielkości) oraz szyfrowania obrazu wirtualnego systemu operacyjnego dostarczanego poprzez sieć LAN lub WAN;
72. Funkcjonalność różnicowego pobierania, aktualizowania spakowanych i zaszyfrowanych obrazów wirtualnego systemu operacyjnego dostarczanego poprzez sieć LAN lub WAN;
73. Mechanizm dostarczania zaszyfrowanych obrazów systemu operacyjnego w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym;
74. Integracja aplikacji zainstalowanych w obrazie wirtualnego systemu operacyjnego z głównym systemem operacyjnym na komputerze - funkcjonalność uruchamiania aplikacji pracujących pod kontrolą systemu wirtualnego z poziomu odnośników zlokalizowanych w menu podręcznym użytkownika na systemie bazowym, z zachowaniem oryginalnego wyglądu i działania aplikacji.

1.2. Pakiet biurowy

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

1. Wymagania odnośnie interfejsu użytkownika:
 - a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na 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 systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
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),
 - c. umożliwia wykorzystanie schematów XML,
 - d. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabelą A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766).
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleczeń, język skryptowy).
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
 - a. Edytor tekstów;
 - b. Arkusz kalkulacyjny;
 - c. Narzędzie do przygotowywania i prowadzenia prezentacji;
 - d. Narzędzie do tworzenia i wypełniania formularzy elektronicznych;
 - e. Narzędzie do tworzenia drukowanych materiałów informacyjnych;
 - f. Narzędzie do tworzenia i pracy z lokalną bazą danych;

- g. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);
 - h. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR;
 - i. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
7. 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 prywatą;
 - 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;
 - r. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.
8. 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.
9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
- a. Przygotowywanie prezentacji multimedialnych, które będą:
 - b. Prezentowanie przy użyciu projektora multimedialnego;
 - c. Drukowanie w formacie umożliwiającym robienie notatek;
 - d. Zapisanie jako prezentacja tylko do odczytu;
 - e. Nagrywanie narracji i dołączanie jej do prezentacji;
 - f. Opatrywanie slajdów notatkami dla prezentera;
 - g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo;
 - h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego;
 - i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym;
 - j. Możliwość tworzenia animacji obiektów i całych slajdów;
 - k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera;
 - l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010;
10. Narzędzie do tworzenia i wypełniania formularzy elektronicznych musi umożliwiać:
- a. Przygotowanie formularza elektronicznego i zapisanie go w pliku w formacie XML bez konieczności programowania;
 - b. Umieszczenie w formularzu elektronicznym pól tekstowych, wyboru, daty, list rozwijanych, tabel zawierających powtarzające się zestawy pól do wypełnienia oraz przycisków;
 - c. Utworzenie w obrębie jednego formularza z jednym zestawem danych kilku widoków z różnym zestawem elementów, dostępnych dla różnych użytkowników;
 - d. Pobieranie danych do formularza elektronicznego z plików XML lub z lokalnej bazy danych wchodzącej w skład pakietu narzędzi biurowych;
 - e. Możliwość pobierania danych z platformy do pracy grupowej;
 - f. Przesłanie danych przy użyciu usługi Web (tzw. web service);
 - g. Wypełnianie formularza elektronicznego i zapisywanie powstałego w ten sposób dokumentu w pliku w formacie XML;
 - h. Podpis elektroniczny formularza elektronicznego i dokumentu powstałego z jego wypełnienia.
11. 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.
12. 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.
13. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
- a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
 - b. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
 - c. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
 - d. Automatyczne grupowanie poczty o tym samym tytule
 - e. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
 - f. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
 - g. Zarządzanie kalendarzem
 - h. Udostępnianie kalendarza innym użytkownikom
 - i. Przeglądanie kalendarza innych użytkowników
 - j. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
 - k. Zarządzanie listą zadań
 - l. Zlecanie zadań innym użytkownikom
 - m. Zarządzanie listą kontaktów
 - n. Udostępnianie listy kontaktów innym użytkownikom
 - o. Przeglądanie listy kontaktów innych użytkowników
 - p. Możliwość przysyłania kontaktów innym użytkownikom
 - q. Posiadać możliwość integracji z wtyczką do systemu HI-Path Expressions.

1.3. Pakiet licencji dostępowych

Pakiet licencji dostępowych musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów:

1. Serwerowych systemów operacyjnych,
2. Serwerów portali wielofunkcyjnych intranet,
3. Serwerów poczty e-mail,
4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem,
5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej,
6. Klienta systemu antywirusowego.

1.4. Serwerowy system operacyjny

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania, co najmniej 8 fizycznych procesorów x64 oraz co najmniej 2 TB pamięci RAM.
2. Wsparcie (na umożliwiającym to sprzęcie) dodawania pamięci RAM bez przerywania pracy.
3. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
4. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów nie wykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
5. Wbudowane wsparcie instalacji i pracy na wolumenach które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,

- b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
- 6. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 7. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- 8. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
- 9. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- 10. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 11. Graficzny interfejs użytkownika.
- 12. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- 13. Możliwość zmiany języka interfejsu dla co najmniej 10 języków.
- 14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
- 15. Obsługa platform sprzętowych x86, x64.
- 16. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu
- 17. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania):
 - a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe),
 - c. Zdalna dystrybucja oprogramowania na stacje robocze,
 - d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
 - e. PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego),
 - f. Szyfrowanie plików i folderów,
 - g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
 - h. Możliwość tworzenia systemów wysokiej dostępności (kastry typu fail-over) oraz rozłożenia obciążenia serwerów,
 - i. Serwis udostępniania stron WWW,
 - j. Serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management),
 - k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - l. Wbudowane usługi VPN pozwalające na zestawienie minimum 500 równoczesnych połączeń i nie wymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na tworzenie maszyn wirtualnych ze zgodnym z platformą sprzętową systemem operacyjnym. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami.
- 18. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta.
- 19. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- 20. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- 21. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
- 22. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

1.5.Oprogramowanie do zarządzania środowiskami serwerowymi

Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 2 fizyczne procesory serwera zarządzanego. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do zarządzania dowolną liczbą środowisk systemu operacyjnego na tym serwerze.

Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

- System zarządzania infrastrukturą i oprogramowaniem
- System zarządzania komponentami
- System zarządzania środowiskami wirtualnym
- System tworzenia kopii zapasowych
- System automatyzacji zarządzania środowisk IT
- System zarządzania incydentami i problemami
- Ochrona antymalware

System zarządzania infrastrukturą i oprogramowaniem

System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji.

1. Inwentaryzacja i zarządzanie zasobami:

- a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania
- b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu
- c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp.)
- d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta
- e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera

1. Użytkowane oprogramowanie – pomiar wykorzystania:

- a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania
 - b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.
2. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

3. Definiowanie i sprawdzanie standardu serwera:

- a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,
- b. Reguły powinny sprawdzać następujące elementy systemu komputerowego:
 - stan usługi (Windows Service)
 - obecność poprawek (Hotfix)
 - WMI
 - rejestr systemowy

- system plików
 - Active Directory
 - SQL (query)
 - Metabase
4. Raportowanie, prezentacja danych:
- a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub
 - b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services
 - c. System powinien posiadać predefiniowane raport w następujących kategoriach:
 - Sprzęt (inventaryzacja)
 - Oprogramowanie (inventaryzacja)
 - Oprogramowanie (wykorzystanie)
 - Oprogramowanie (aktualizacje, w tym system operacyjny)
 - d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport
 - e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu
5. Analiza działania systemu, logi, komponenty
- a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy
 - b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura
 - a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być dostępne dla klientów systemu w celu automatycznej konfiguracji.
 - b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
 - c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
 - d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
 - e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
 - f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
 - g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
 - h. Wsparcie dla protokołu IPv6.
 - i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.
2. Audyt zdarzeń bezpieczeństwa

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:

- a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie” rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).
 - b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.
 - c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst” – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.
3. Konfiguracja i monitorowanie
- System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:
- a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:
 - rejestru
 - WMI
 - OLEDB
 - LDAP
 - skrypty (uruchamiane w celu wykrycia atrybutów obiektu),
 W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.
 - b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp.
 - c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp. elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:
 - Windows Server 2003/2008/2008R2
 - Active Directory 2003/2008
 - Exchange 2003/2007/2010
 - Microsoft SharePoint 2003/2007/2010
 - Microsoft SharePoint Services 3.0
 - Microsoft SharePoint Foundation 2010
 - SQL 2005/2008/2008R2 (x86/x64/ia64)
 - Windows Client OS (XP/Vista/7)
 - Information Worker (Office, IExplorer, Outlook, itp...)
 - IIS 6.0/7.0/7.5
 - HP-UX 11i v2/v3
 - Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86)
 - Red Hat Enterprise Linux 4/5/6 (x86/x64) Server
 - Novell SUSE Linux Enterprise Server 9/10SP1/11
 - IBM AIX v5.3 i v6.1/v7.1 (POWER)
 - d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.
 - e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:
 - interfejsy sieciowe
 - porty
 - sieci wirtualne (VLAN)
 - grupy Hot Standby Router Protocol (HSRP)
 - f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
 - SNMP (trap, probe)
 - WMI Performance Counters
 - Log Files (text, text CSV)
 - Windows Events (logi systemowe)

- Windows Services
 - Windows Performance Counters (perflib)
 - WMI Events
 - Scripts (wyniki skryptów, np.: WSH, JSH)
 - Unix/Linux Service
 - Unix/Linux Log
- g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów
4. Tworzenie reguł
- a. w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:
- Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event)
 - Performance based (SNMP performance, WMI performance, Windows performance)
 - Probe based (scripts: event, performance)
- b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.
- c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:
- na ilość takich samych próbek o takiej samej wartości
 - na procentową zmianę od ostatniej wartości próbki.
- d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia” się monitorowanego parametru w zakresie przebiegu bazowego „baseline” w zadanym okresie czasu.
- e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.
- f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:
- ASP .Net Application
 - ASP .Net Web Service
 - OLE DB
 - TCP Port
 - Web Application
 - Windows Service
 - Unix/Linux Service
 - Process Monitoring
- Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji.
- g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.
- h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp...) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).
- i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.
- j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostępność), i licznika wydajności (z agregacją dla wartości – min, max, avg).
5. Przechowywanie i dostęp do informacji
- a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp.) powinny być przechowywane w bazie danych operacyjnych.

- b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.
 - c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).
 - d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystane w celu rozszerzenia tej funkcjonalności.
 - e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.
 - f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:
 - XML
 - CSV
 - TIFF
 - PDF
 - XLS
 - Web archive
6. Konsola systemu zarządzania
- a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.
 - b. System powinien udostępniać dwa rodzaje konsoli:
 - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna)
 - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).
 - c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:
 - Alerts
 - Events
 - State
 - Performance
 - Diagram
 - Task Status
 - Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).
 - d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.
 - e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdują (po typie, ważności, typach obiektów, itp.), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych”.
 - f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.
 - g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
 - opcji definiowania ról użytkowników
 - opcji definiowania widoków
 - opcji definiowania i generowania raportów
 - opcji definiowania powiadomień
 - opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących
 - opcji instalacji/deinstalacji klienta.

- h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).
- 7. Wymagania dodatkowe
 - a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:
 - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
 - Wykonywanie operacji w systemie z poziomu linii poleceń,
 - Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
 - Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie,

System zarządzania środowiskami wirtualnym

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura

a. System zarządzania środowiskiem wirtualnym powinien składać się z:

- serwera zarządzającego,
- relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
- konsoli, instalowanej na komputerach operatorów,
- portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
- biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
- agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
- „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).

c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.

2. Interfejs użytkownika

- a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.
- b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.
- c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp.
- d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres użycia procesora i podgląd na pulpit.
- e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.

3. Scenariusze i zadania

a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:

- 1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
- 2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:
 - profilu sprzętowego
 - profilu systemu operacyjnego,
 - przygotowanych dysków twardych,

b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.

- c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:
 - w trybie migracji „on-line” – bez przerywania pracy,
 - w trybie migracji „off-line” – z zapisem stanu maszyny
 - d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.
 - e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.
 - f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance” w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.
 - g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
 - h. System musi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.
4. Wymagania dodatkowe
- a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.
 - b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczny bez potrzeby każdorazowego potwierdzania.
 - c. System musi kreować raporty z działania zarządzanego środowiska, w tym:
 - utylizacja poszczególnych hostów,
 - trend w utylizacji hostów,
 - alokacja zasobów na centra kosztów,
 - utylizacja poszczególnych maszyn wirtualnych,
 - komputery-kandydaci do wirtualizacji
 - d. System musi umożliwiać skorzystanie z szablonów:
 - wirtualnych maszyn
 - usług
 oraz profili dla:
 - aplikacji
 - serwera SQL
 - hosta
 - sprzętu
 - systemu operacyjnego gościa
 - e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).
 - f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.
 - g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją).

System tworzenia kopii zapasowych

System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania:

1. System musi składać się z:
 - a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
 - b. agentów kopii zapasowych instalowanych na komputerach zdalnych
 - c. konsoli zarządzającej
 - d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach
 - e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną

- f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
2. System kopii zapasowych musi umożliwiać:
 - a. zapis danych na puli magazynowej złożonej z dysków twardych
 - b. zapis danych na bibliotekach taśmowych
3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej.
4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.
7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
8. System kopii zapasowych powinien umożliwiać przywrócenie:
 - a. danych plikowych
 - b. danych aplikacyjnych
 - c. stanu systemu (Systemstate)
 - d. obrazu systemu operacyjnego (tzw. Bare Metal Restore)
9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych
10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości.
11. Agenci systemu kopii zapasowych muszą posiadać konfigurację dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy.
12. System kopii zapasowych musi rozpoznawać aplikacje:
 - a. ze względu na tworzone logi transakcyjne:
 - Microsoft Exchange Server
 - Microsoft Office Sharepoint Server
 - Microsoft SQL Server
 - b. ze względu na zapewnienie nieprzerwalności pracy
 - Microsoft Virtual Server 2005
 - Microsoft Hyper-V server
13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach.
14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach.
15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów.
16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń.
17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje”.
18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych.
19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych.
20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku.
22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat.

23. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe.
25. System kopii zapasowych musi umożliwiać odtworzenie danych do:
 - a. lokalizacji oryginalnej
 - b. lokalizacji alternatywnej
 - c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.

1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.
2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.
3. System musi wspomagać planowanie i automatyzację wdrażania poprawek.
4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych.
5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania workflow.
6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem.
7. Wbudowane (gotowe) workflow, takie jak:
 - Active Directory Password Reset
 - Microsoft Cluster Patching
 - Microsoft SQL Server Cluster Patching
 - Microsoft SQL: Server Dump Copy Load
 - Operations Manager Event Remediation
 - Operations Manager Event Remediation and Enrichment
 - Operations Manager Service Alert Testing
 - VM Provisioning
 - Working with FTP
 - Operations Manager Tool Integration
 - Operations Manager: Manager of Managers
 - Operations Manager: Maintenance Windows
 - Active Directory: New Employee Onboarding
 - Operations Manager: Multi-Service Desk Integration

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi spełniać następujące wymagania:

1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna)
2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.

4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
 - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
 - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
 - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
 - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
 - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
 - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
 - Tworzenie baz wiedzy na temat rozwiązywania problemów,
 - Automatyzację działań w przypadku znanych i opisanych problemów,
 - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

Ochrona antymalware

Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploit zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem.
3. Centralne zarządzanie politykami ochrony.
4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Zastosowanie kilku skanerów antywirusowych różnych producentów na jednej platformie.
7. Możliwość wyboru aktywnych silników skanujących.
8. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów”, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
9. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
10. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
11. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa”, itd.).
12. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów.

Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.

13. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.
14. Możliwość natywnego współdziałania z systemami typu „rights-management”
15. Możliwość filtrowania i blokowania zabronionych przez polityki treści czy słów kluczowych.

1.6. Serwer poczty elektronicznej typ I

Serwer obsługi poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
 - a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
 - b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
 - c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
 - d. 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
 - e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:
 - a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości
 - b. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
 - c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
 - d. 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
 - e. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania
 - f. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
 - g. Obsługa list i grup dystrybucyjnych.
 - h. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
 - i. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalanie harmonogramu.
 - j. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
 - k. Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
 - l. 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.
 - m. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwanie pliku dźwiękowego.
 - n. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
 - o. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
 - p. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.

- q. Dla klientów poczty z pakietu biurowego (punkt 1.2 powyżej) powinien wspierać konektor systemu HI-Path Expressions.
- 3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
 - a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja
 - b. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.
 - c. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
 - d. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
 - e. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
 - f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
 - g. Integracja z usługami zarządzania dostępem do treści (AD RMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.
 - h. Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami AD RMS.
 - i. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
 - j. Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
- 4. Wsparcie dla użytkowników mobilnych:
 - a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
 - b. Możliwość „lekkiej” synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
 - c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
 - d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
 - e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
 - f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

1.7. Serwer poczty elektronicznej typ II

Serwer systemu poczty elektronicznej typ II musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
 - a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
 - b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
 - c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
 - d. 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
 - e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:
 - a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości
 - b. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
 - c. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
 - d. 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
 - e. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania
 - f. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
 - g. Obsługa list i grup dystrybucyjnych.
 - h. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów.
 - i. Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalanie harmonogramu.
 - j. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
 - k. Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
 - l. 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, wysłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
 - m. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwanie pliku dźwiękowego.
 - n. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
 - o. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
 - p. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.
3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
 - a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja
 - b. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.
 - c. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych.
 - d. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.

- e. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
 - f. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami.
 - g. Integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania.
 - h. Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
 - i. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
 - j. Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
4. Wsparcie dla użytkowników mobilnych:
- a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu opisanej w punkcie a). Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem
 - b. Możliwość „lekkiej” synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
 - c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
 - d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej
 - e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.
 - f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.
5. Funkcje związane z niezawodnością systemu:
- a. Rezygnacja z wdrażania złożonych i kosztownych rozwiązań obsługi klastrowania oraz produktów do replikacji danych firm zewnętrznych w celu zapewnienia pełnej redundancji oprogramowania Exchange.
 - b. Automatyzacja replikacji bazy danych i przełączania awaryjnego już z dwoma serwerami, a także w wypadku centrów danych rozproszonych geograficznie.
 - c. Utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki maksymalnie 16 zarządzanym przez Exchange replikom każdej bazy danych skrzynki pocztowej.
 - d. Ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, co pozwala na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej.
 - e. Zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.

1.8.Serwer komunikacji wielokanałowej typ I

System oparty na funkcjonalności serwera komunikacji wielokanałowej (SKW) typ I wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

1. Prosta, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video
2. Przesyłanie wiadomości tekstowych z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę oraz urządzeń mobilnych bazujących na Windows Mobile.
3. Możliwość telekonferencji

Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty e-mail, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać natywną integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu:

1. Ujednolicenie komunikacji biznesowej
 - a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
 - b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności.
 - c. Dostępność aplikacji klienckiej udostępniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc.
 - d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością:
 - 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
 - Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji
 - e. Dostępność funkcjonalności text-to-speech w języku polskim
 - f. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
 - g. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
 - h. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym.
 - i. Usługi bezpieczeństwa umożliwiające chronioną komunikację wewnątrz organizacji.
 - j. Aplikacje biznesowe dostępne bezpośrednio na urządzeniach mobilnych.
 - k. Mobilny dostęp do ludzi i danych firmowych.
 - l. Obniżone koszty dzięki zdalnej administracji i zarządzaniu urządzeniami.
 - m. Niższe koszty usług telefonicznych i komunikacji między odległymi lokalizacjami.
 - n. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
 - o. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich.
2. W związku z tak postawionymi założeniami SKW ma zapewnić:
 - a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników.
 - b. Ulepszoną komunikację poprzez wykorzystanie statusu obecności i konferencje w czasie rzeczywistym.
 - c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami.

- d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych.
- 3. SKW ma zapewnić obsługę następujących funkcjonalności:
 - a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności.
 - b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.
 - c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi, możliwość realizacji połączeń głosowych do i z sieci PSTN (publicznej sieci telefonicznej). Możliwość realizacji funkcjonalności RCC (Remote Call Control) tj. zarządzania telefonem stacjonarnym firm trzecich z poziomu komunikatora.
 - d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych.
 - e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu.
 - f. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników.
 - g. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie z poziomu serwera WWW.
 - h. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
 - i. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.
 - j. Wbudowane funkcjonalności: SIP Proxy
 - k. Wbudowana funkcjonalność mostka konferencyjnego MCU
 - l. Obsługa standardów: CSTA, TLS, SIP over TCP
 - m. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów
 - n. Mechanizm pozwalający na przełączenie serwera w tryb off-line (np. w celach dokonania czynności administracyjnych) bez utraty usług serwera dla zalogowanych użytkowników, a jednocześnie blokujący dostęp nowych użytkowników
 - o. Możliwość administrowania z wiersza poleceń
 - p. Możliwość administrowania za pomocą interfejsu Web
 - q. Mechanizm gotowych kreatorów (wizard) umożliwiających planowanie i zmiany topologii serwerów SKW
 - r. Wykorzystanie wyłącznie 64 bitowej platformy serwerowego systemu operacyjnego
 - s. Możliwość instalacji w układzie klastra niezawodnościowego.
 - t. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów.

1.9. Serwer zapory ogniowej

Serwer zapory ogniowej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

- Filtrowanie ruchu internetowego na poziomie pakietów, połączeń i aplikacji
- Filtrowanie stateful inspection
- Nielimitowane filtrowanie w warstwie aplikacji ruchu VPN, HTTP, FTP, SMTP, POP3, DNS, H.323, RPC
- Możliwość filtrowania URLi zawierających niepożądane treści

- Natywna integracja z mechanizmami skanowania ruchu SMTP
- Publikowanie aplikacji przy wykorzystaniu kreatorów i pozwalające na zabezpieczenie serwerów Web, serwerów poczty elektronicznej oraz aplikacji handlu elektronicznego przed atakami z zewnątrz.
- Ochrona udostępnianych zasobów przez protokół HTTPS (możliwość terminowania i skanowania filtrami aplikacyjnymi ruchu w kanale SSL)
- Możliwość inspekcji szyfrowanych sesji HTTPS zgodnie z ustalonymi regułami
- Analizowanie ruchu zaszyfrowanego przy wykorzystaniu mostkowania SSL – SSL
- Rozszerzony zakres translacji adresów (NAT) umożliwiający publikowanie serwerów poczty elektronicznej na bazie 1-do-1 NAT
- Wsparcie dla technologii VoIP
- Automatyczna translacja łączy
- Wbudowany moduł wykrywania włamań
- VPN gateway bez limitu połączeń VPN. Możliwość budowania tuneli VPN od klientów oraz połączeń VPN site-to site a także tworzenia kwarantany VPN.
- Integracja z usługą katalogową Active Directory i możliwość uwierzytelniania użytkowników domeny,
- Współpraca ze standardami RADIUS, RADIUS OTP, SecurID,
- Wbudowane formularze uwierzytelniające. Format formularzy powinien dawać możliwość modyfikacji i graficznego dostosowania do wymagań użytkownika.
- Uwierzytelnianie użytkownika przed dostępem do serwerów aplikacyjnych
- Wykorzystanie mechanizmu pojedynczego logowania w oparciu o Active Directory,
- Możliwość delegacji poświadczeń użytkownika przy korzystaniu z chronionych zasobów
- Wbudowany bufor http – Proxy
- Możliwość definiowania reguł buforowania
- Ochrona przed popularnymi typami ataków (co najmniej: Flood, SYN Attack, DoS http, DoS non-TCP, UDP flood)
- System monitorowania w trybie rzeczywistym z możliwością składowania logów w plikach testowych bądź relacyjnej bazie danych
- System skanowania stron internetowych pod kątem obecności wirusów i malware
- System raportowania z możliwością generowania powiadomień i ich dystrybucji
- Licencjonowanie per procesor bez ograniczenia liczby użytkowników VPN
- Skalowalność rozwiązania
- Obsługa nielimitowanej liczby procesorów serwera
- Możliwość instalacji na farmie serwerów, w tym w układzie NLB.

1.10.Serwer wewnętrznego portalu wielofunkcyjnego

Serwery portali wielofunkcyjnych (PW) muszą umożliwiać użytkownikom sieci intranet poprzez wbudowane mechanizmy:

1. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z wykorzystaniem praw dostępu na bazie usługi katalogowej,
2. Wykorzystanie serwera relacyjnej bazy danych jako miejsca składowania danych portalu,
3. Publikację dokumentów i treści na witrynach,
4. Udostępnienie formularzy elektronicznych,
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. Analizy danych wraz z graficzną prezentacją danych,

13. Możliwość wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning).

Serwery PW muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.

PW 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 PW muszą posiadać następujące cechy dostępne bezpośrednio, jako natywne właściwości produktu:

1. Interfejs użytkownika:

- a. 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).
- b. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
- c. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
- d. Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu
- e. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji uproszczonej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).

2. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:

- a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili
 - b. 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
 - c. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
 - d. Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony)
 - e. 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
 - f. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
 - g. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
 - h. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym.
- #### 3. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:
- a. Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.
 - b. Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML)
 - c. Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego

- d. Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów
- e. Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte
- f. Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana
- g. Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny).
- h. Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo,
- 4. Organizacja i publikacja treści:
 - a. Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.
 - b. Zastosowanie procesów zatwierdzania zawartości przez publikację, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.
 - c. Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.
 - d. Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię. Automatyczne generowanie mapy stron portalu.
 - e. Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.
 - f. Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.
 - g. Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.
 - h. Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.
 - i. Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu.
- 5. Repozytoria dokumentów:
 - a. Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów
 - b. Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa
 - c. Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu
 - d. Możliwość publikacji plików w strukturze katalogów

- e. Możliwość publikacji materiałów wideo oraz audio
 - f. Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku
 - g. Możliwość nawigacji po repozytorium dokumentów w oparciu o metadane z metryk dokumentów,
 - h. Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania
 - i. Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x... 2.0), automatyczna kontrola wersji przy publikacji dokumentów
 - j. Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu
 - k. Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.
 - l. Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.
6. Wyszukiwanie treści:
- a. Pełno tekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.
 - b. Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu
 - c. Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, dat publikacji
 - d. Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów
 - e. Możliwość definiowania słownika słów wykluczonych (często używanych)
 - f. Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu
 - g. Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.
 - h. Przedstawianie w wynikach duplikatów plików
 - i. Statystyki wyszukiwanych fraz
7. Administracja intranetem i inne funkcjonalności
- a. Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, nie wymagająca szczególnych kompetencji technicznych
 - b. Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu
 - c. Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści
 - d. Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu
 - e. Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów,
 - f. Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu

- g. Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy
- h. Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń
- i. Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.
- j. Funkcjonalność definiowania procesów obiegu dokumentów (workflow) przy wykorzystaniu prostych w obsłudze narzędzi portalu.

1.11.Serwer wielofunkcyjnego portalu Internetowego

Serwery wielofunkcyjnych portali Internetowych (WPI) muszą umożliwiać użytkownikom sieci internet poprzez wbudowane mechanizmy:

1. Publikację dokumentów, treści i materiałów multimedialnych na witrynach,
2. Zarządzanie strukturą portalu i treściami WWW,
3. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z wykorzystaniem praw dostępu na bazie usługi katalogowej,
4. Uczestnictwo Internautów w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści,
5. Udostępnienie formularzy elektronicznych,
6. Tworzenie repozytoriów wzorów dokumentów,
7. Tworzenie repozytoriów dokumentów,
8. Wspólną, bezpieczną pracę nad dokumentami,
9. Wersjonowanie dokumentów (dla wersji roboczych),
10. Podpisywanie dokumentów,
11. Organizację pracy grupowej,
12. Wyszukiwanie treści,
13. Dostęp do danych w relacyjnych bazach danych,
14. Analizy danych wraz z graficzną prezentacją danych,
15. Możliwość wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning).

Serwery WPI muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór WIELU niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.

PW muszą udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu publikacji treści, zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów, oraz umożliwić współpracę pomiędzy zespołami złożonych również z osób z poza organizacji oraz z jednostek stowarzyszonych.

Serwery WPI muszą posiadać następujące cechy dostępne bezpośrednio, jako natywne właściwości produktu:

1. Interfejs użytkownika:
 - a. Zarządzanie strukturą portalu, rolami użytkowników, uprawnieniami, okresem publikacji treści, tworzenie artykułów
 - b. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji opisanego w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).
 - c. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów
 - d. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego
 - e. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji uproszczonej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).

2. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
 - a. Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili, również do użytkowników z Internetu,
 - b. Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili
 - c. Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony)
 - d. 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
 - e. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services
 - f. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.
 - g. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym.
3. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:
 - a. Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.
 - b. Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML)
 - c. Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego
 - d. Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów
 - e. Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte
 - f. Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana
 - g. Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny).
 - h. Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo,
4. Organizacja i publikacja treści:
 - a. Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.
 - b. Zastosowanie procesów zatwierdzania zawartości przed publikacją, tzn. udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed udostępnieniem jej wszystkim użytkownikom intranetu.

- c. Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.
 - d. Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię. Automatyczne generowanie mapy stron portalu.
 - e. Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.
 - f. Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.
 - g. Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.
 - h. Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.
 - i. Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu.
5. Repozytoria dokumentów:
- a. Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów
 - b. Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa
 - c. Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu
 - d. Możliwość publikacji plików w strukturze katalogów,
 - e. Możliwość publikacji materiałów wideo oraz audio,
 - f. Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku,
 - g. Możliwość nawigacji po repozytorium dokumentów w oparciu o metadane z metryk dokumentów,
 - h. Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania
 - i. Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x... 2.0), automatyczna kontrola wersji przy publikacji dokumentów
 - j. Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu
 - k. Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.
 - l. Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.
6. Wyszukiwanie treści:
- a. Pełno tekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.
 - b. Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu,
 - c. Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, dat publikacji,

- d. Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów
- e. Możliwość definiowania słownika słów wykluczonych (często używanych)
- f. Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu
- g. Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.
- h. Przedstawianie w wynikach duplikatów plików
- i. Statystyki wyszukiwanych fraz
- 7. Administracja intranetem i inne funkcjonalności
 - a. Możliwość definiowania ról / grup uprawnień w ramach, których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych,
 - b. Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu
 - c. Generowanie powiadomień pocztą elektroniczną dla użytkowników z informacją o publikacji najbardziej istotnych treści
 - d. Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu
 - e. Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów,
 - f. Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu
 - g. Statystyki odwiedzin poszczególnych części i stron portalu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy
 - h. Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie portalu do celów pracy działów i zespołów zadaniowych, które będą mogły być złożone z użytkowników będących pracownikami organizacji Zamawiającego oraz jednostek stowarzyszonych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń
 - i. Funkcjonalność publikowania na portalu formularzy elektronicznych XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.
 - j. Funkcjonalność definiowania procesów obiegu dokumentów (workflow) przy wykorzystaniu prostych w obsłudze narzędzi portalu.

1.12. Serwer relacyjnej bazy danych

Serwer relacyjnej bazy danych (RBD) licencjonowany na core procesora musi spełniać poniższe wymagania poprzez wbudowane mechanizmy:

1. Możliwość szyfrowania przechowywanych danych
System RBD musi pozwalać na szyfrowanie przechowywanych danych. Szyfrowanie musi być cechą systemu RBD i nie może wymagać jakichkolwiek zmian w aplikacjach korzystających z danych. Zasyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zasyfrowana.
2. Kompresja kopii zapasowych
System RBD powinien pozwalać na kompresję kopii zapasowej danych (*backup*) od razu w czasie jej tworzenia. Powinna to być cecha RBD niezależna od systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
3. Ograniczenie użycia zasobów

System powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, pamięć). Reguły definiujące ograniczenia użytkowników lub ich grup w wykorzystaniu zasobów powinny mieć możliwość użycia w nich logiki zaimplementowanej za pomocą języka programowania (np. używanego w danym RBD języka SQL)

4. Korzystanie z zewnętrznych urządzeń do przechowywania kluczy szyfrujących

RBD powinien posiadać mechanizm pozwalający na i przechowywanie kluczy szyfrujących na urządzeniach zewnętrznych (np. czytniki kart). Rozwiązanie to powinno być otwarte, to znaczy pozwalać na dodawanie w przyszłości obsługi urządzeń nowych, oczywiście pod warunkiem dostarczenia przez producenta urządzenia odpowiednich modułów oprogramowania zgodnych z RBD.

5. Skalowalność systemu

System RBD powinien wspierać skalowanie w kontekście wielkości rozwiązania (powinien być dostępny zarówno na platformie wielo-serwerowej, jak również średniej wielkości komputerów i urządzeń mobilnych).

6. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie

Wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników lub zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników).

7. Możliwość definiowania zasad administracyjnych dla serwera lub grupy serwerów

System RBD powinien mieć możliwość automatyzacji zadań administracyjnych przez definiowanie reguł wymuszanych potem przez system. Przykłady takich reguł:

- uniemożliwienie użytkownikom tworzenia obiektów (np. tabel, procedur, baz danych, widoków) o zdefiniowanych przez administratora nazwach lub ich fragmentach

Powinna być możliwa rejestracja i raportowanie niezgodności ze wskazanymi regułami działającego systemu bez wpływu na jego funkcjonalność.

Reguły mogą dotyczyć serwera lub grupy serwerów.

8. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym

System RBD powinien pozwalać na definiowanie rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych bez ujemnego wpływu na wydajność rozwiązania. Przykłady takich zdarzeń to:

- odczyt lub zapis danych na dysku dla wyszczególnionego zapytania (w celu wychwytywania zapytań znacząco obciążających system)
- wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur)
- para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy takim jak np. tabela (w celu wychwytywania długotrwałych blokad obiektów bazy)

Rejestracja zdarzeń powinna pozwalać na selektywne ich wychwytywanie (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu)

9. Możliwość rejestracji zmiany w rekordzie danych

System powinien pozwalać na rejestrację zmian w danych włącznie z zapamiętaniem stanu pojedynczego rekordu danych sprzed modyfikacji. Rozwiązanie nie powinno ujemnie wpływać na wydajność systemu i powinno być konfigurowalne bez wpływu na istniejące aplikacje korzystające z danych. Rozwiązanie powinno rejestrować także zmiany w definicji struktur danych (np. zmiany schematu tabeli)

10. Audyt dostępu do danych

System RBD powinien pozwalać na rejestrację operacji takich jak: logowanie, wylogowanie użytkownika, zmiany w definicji obiektów bazy danych (tabele, procedury), wykonywanie przez wskazanego użytkownika operacji takich jak SELECT, INSERT, UPDATE, DELETE. Rozwiązanie powinno być niezależne od aplikacji, wbudowane w RBD.

11. Zarządzanie serwerem za pomocą skryptów

System RBD powinien udostępniać mechanizm zarządzania silnikiem bazy danych za pomocą skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.

12. Możliwość dodawania procesorów bez restartu systemu

System RBD powinien umożliwiać dodanie procesora do systemu bez konieczności restartu silnika bazy danych.

13. Możliwość dodawania pamięci bez restartu systemu

System RBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych.

14. Możliwość wywoływania procedur składowanych jako usług sieci Web (WebServices)

15. System RBD powinien umożliwiać tworzenie procedur składowanych które mogą być udostępnione i wywoływane jako *WebServices* bez wykorzystania dodatkowego oprogramowania.

16. Kopie bazy tylko do odczytu

System powinien umożliwiać tworzenie w dowolnym momencie kopii tylko do odczytu bazy danych z bieżącego momentu czasu. Wiele takich kopii może być równolegle użytkowanych w celu wykonywania z nich zapytań.

17. Wysoka dostępność realizowana programowo z korekcją błędów pamięci masowej

System RBD powinien posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:

- bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam RBD)
- niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe)
- klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach
- czas przełączenia na system zapasowy poniżej 10 sekund.
- brak limitu odległości między systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza)
- kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenia sieci)
- system automatycznie naprawia błędy pamięci masowej (w przypadku odkrycia błędu fizycznego odczytu danych z pamięci masowej, poprawny fragment danych jest transferowany z drugiego systemu i korygowany)

System RBD powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsięciach komputerowych.

18. Wykonywanie typowych zadań administracyjnych w trybie on-line

System RBD powinien umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy (operacje w trybie on-line).

19. Możliwość automatycznej aktualizacji systemu

System RBD powinien umożliwiać automatyczne ściąganie i instalację wszelkich poprawek (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).

20. Definiowanie nowych typów danych w RBD

System RBD powinien umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojonych typów wbudowanych lub ich kombinacji.

21. Wsparcie dla technologii XML

System RBD powinien udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML.

W szczególności powinien:

- udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli

- udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD
 - udostępniać język zapytań do struktur XML
 - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML)
 - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań
22. Obsługa błędów w kodzie zapytań
Język zapytań i procedur w systemie RBD powinien umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
23. Możliwość tworzenia rekursywnych zapytań do bazy danych
System RBD powinien udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
24. Replikacja danych i modyfikacja w wielu punktach
System RBD powinien pozwalać na transakcyjną replikację wybranych danych z bazy danych między wieloma węzłami. Dodanie lub usunięcie węzła nie powinno wpływać na funkcjonowanie i spójność systemu replikacji ani nie powinno przerywać procesu replikacji. Dane mogą w takim schemacie replikacji być modyfikowane w dowolnym węźle (ale tylko w jednym węźle w danym momencie). System powinien zawierać narzędzie do nadzorowania i wizualizacji topologii oraz stanu procesu replikacji.
Dodatkowo system RBD powinien umożliwiać kompresję przesyłanych danych między serwerami uczestniczącymi w replikacji, aby minimalizować obciążenie łączy sieciowych.
25. Indeksowanie podzbioru danych w tabeli
System RBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.
26. Dedykowana sesja administracyjna
System RBD powinien pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
27. Partycjonowanie danych
System powinien pozwalać na podział danych w jednej tabeli między różne fizyczne pamięci masowe zgodnie ze zdefiniowanymi warunkami podziału.
System RBD powinien udostępniać mechanizm równoległego (wielowątkowego) dostępu do danych umieszczonych w różnych partycjach.
Dodatkowo powinna być dostępna możliwość szybkiego przesyłania dużych zbiorów danych poprzez mechanizm przełączania partycji (czyli dane przenoszone są z jednej tabeli do drugiej za pomocą operacji na metadanych, a nie przez fizyczne kopiowanie rekordów). Dzięki takiej funkcjonalności możliwe jest przeniesienie dużej liczby rekordów w bardzo krótkim czasie (rzędu sekund). Dodatkowo minimalizowane jest odczuwanie wpływu tej operacji przez użytkowników (minimalny wpływ przenoszenia danych na obciążenie systemu).
28. Wsparcie dla danych przestrzennych
System RBD powinien zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
- zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
 - powinien oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.
 - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu RBD,

- typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.),
- 29. Możliwość efektywnego przechowywania dużych obiektów binarnych
System RBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty, itp.) Obiekty te powinny nie powinny być przechowywane w plikach bazy danych, ale w systemie plików. Jednocześnie pliki te powinny być zarządzane przez RBD (kontrola dostępu na podstawie uprawnień nadanych w RBD). Dodatkowo dane binarne powinny być dostępne dla użytkowników bazy danych jako standardowa kolumna tabeli (dostęp z poziomu zapytań języka SQL obsługiwanego przez RBD).
- 30. Możliwość kompresji przechowywanych danych
System RBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych. Ze względu na to, że wydajność serwerów baz danych w największym stopniu ograniczana jest przez podsystemy dyskowe, zastosowanie kompresji danych pozwoli osiągnąć lepszą wydajność przy nie zmienionej konfiguracji sprzętowej (skompresowane dane zajmują mniej miejsca, a skoro zajmują mniej miejsca, to ich odczytanie zajmuje mniej zasobów). System kompresji powinien umożliwiać również kompresję UNICODE systemem UCS-2.
- 31. Raportowanie zależności między obiektami
System RBD powinien udostępniać obiekty systemowe do raportowania zależności między obiektami baz danych. Mechanizm ten powinien umożliwiać m.in. uzyskanie informacji o referencjach między obiektami, czyli które obiekty bazy danych odwołują się do innych obiektów.
- 32. Mechanizm blokowania planów wykonania zapytań do bazy danych
System RBD powinien udostępniać mechanizm pozwalający na zablokowanie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Ma to istotne znaczenie m.in. w przypadku przenoszenia systemów między serwerami (środowisko testowe i produkcyjne), migracji do innych wersji RBD lub wprowadzania zmian sprzętowych w serwerach. Dzięki mechanizmom blokady planów wykonania zapytań czas odpowiedzi na zapytania staje się bardziej przewidywalny.
- 33. Efektywne zarządzanie pustymi wartościami w bazie danych
System RBD powinien efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
- 34. Wsparcie dla optymalizacji zapytań z modelu gwiazdy (fakty-wymiary)
System RBD powinien udostępniać mechanizmy optymalizacji zapytań w modelu gwiazdy (tabela faktów łączona z tabelami wymiarów). Zapytania te często wykorzystywane są w hurtowniach danych i analizach wielowymiarowych. Ze względu na dużą liczbę danych wykorzystywanych w tego typu zapytaniach metody optymalizacji tego typu zapytań pozwalają znacząco zwiększyć wydajność przy tworzeniu rozwiązań hurtowni danych i wielowymiarowych struktur analitycznych (OLAP).
- 35. Wsparcie dla Indeksów kolumnowych
System RBD powinien umożliwiać tworzenie indeksów przechowujących dane osobno dla każdej z kolumn tabeli łącząc je następnie w całość. Indeks powinien również wykorzystywać mechanizm kompresji.
- 36. Wsparcie dla zapytań aktualizujących tabele faktów w modelach wielowymiarowych
System RBD powinien udostępniać wbudowane mechanizmy pozwalające w łatwy i szybki sposób aktualizować zawartość tabel faktów (wykorzystywanych w modelach wielowymiarowych). Mechanizm ten powinien być dostępny z poziomu zapytań języka SQL obsługiwanego przez silnik bazy danych.
- 37. System transformacji danych

System powinien posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Zestaw standardowych dostępnych transformacji powinien obejmować takie transformacje jak: sortowanie, wyszukiwanie wartości według klucza w tabelach słownikowych, automatyczna obsługa SCD (*Slowly Changing Dimension*) w zasilaniu hurtowni danych, pobranie danych z serwera FTP, wysłanie e-maila, łączenie danych z wykorzystaniem logiki rozmytej, poprawa jakości danych wykorzystująca integrację z dedykowanym systemem zarządzania jakością danych oraz jego bazą wiedzy i reguł walidujących. Powinna być także zapewniona możliwość tworzenia własnych transformacji.

Środowisko tworzenia transformacji danych powinno udostępniać m.in.

- mechanizm debuggowania tworzonego rozwiązania,
 - mechanizm stawiania „pułapek” (breakpoints),
 - mechanizm logowania do pliku wykonywanych przez transformację operacji,
 - możliwość wznowienia wykonania transformacji od punktu, w którym przzerwano jej wykonanie (np. w wyniku pojawienia się błędu),
 - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
 - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
 - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
 - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
 - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiiany źródła danych,
- Wykonywane transformacje danych powinny mieć możliwość integracji z transakcjami bazy danych RBD, także rozproszonymi (transakcje obejmujące bazy na różnych fizycznych serwerach RBD) bez potrzeby pisania kodu.

38. System analityczny

System powinien posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych).

System powinien umożliwiać pracę w dwóch trybach:

- wielowymiarowym (tworzenie kostek wielowymiarowych)
- tabelarycznym (wykorzystującym technologię in-memory BI).

Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.

System powinien mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłączenie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna powinna mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Agregacje powinny być przeliczane niezależnie dla każdego modelu składowania w jednej bazie.

System powinien pozwalać na integrację z RBD –wymagana jest możliwość uruchomienia procesu wyliczenia agregacji zainicjowana poprzez dodanie rekordu do tabeli w RBD.

Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).

System powinien pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron WWW powiązanych z przeglądany obszarem kostki).

System powinien posiadać narzędzie do rejestracji i śledzenia wykonywanych zapytań spójne z analogicznym narzędziem dla systemu RBD.

System powinien umożliwiać rejestrowanie zapytań wykonywanych przez użytkowników, a następnie umożliwiać na podstawie zgromadzonych informacji na automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).

System powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).

System powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.

System powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.

System powinien umożliwiać użytkownikom tworzenie analiz In-Memory, czyli przetwarzanie dużej liczby rekordów skompresowanych w pamięci RAM. Powinien umożliwiać tworzenie modeli wykorzystujących tabele pochodzące z wielu niezależnych źródeł danych i łączone między sobą relacjami.

System powinien udostępniać dedykowany język do tworzenia logiki biznesowej w modelu. Język ten powinien m.in. obsługiwać relacje utworzone między tabelami, mechanizmy time intelligence (operacje na datach i okresach) oraz zapewniać mechanizmy kontroli bezpieczeństwa i dostępu do danych na poziomie poszczególnych wierszy.

System powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane).

System powinien mieć wbudowaną funkcję importu tabelarycznych modeli danych wykorzystujących technologię in-memory BI i przygotowanych w aplikacji Microsoft Excel. Podczas procesu importu na serwerze model powinien być odtwarzany w postaci bazy danych. System powinien umożliwiać zasilanie modelu tabelarycznego m.in. z następujących systemów źródłowych: bazy relacyjne, bazy wielowymiarowe, modele tabelaryczne, zbiory danych przechowywane w usługach chmury publicznej, pliki płaskie, inne raporty udostępniane w formacie Atom 1.0.

System powinien umożliwiać działanie modelu tabelarycznego w dwóch trybach – z użyciem buforowania (możliwe opóźnienie, ale większa wydajność) oraz bez użycia buforowania (zapytania użytkowników końcowych korzystających z modelu są przesyłane bezpośrednio do źródłowej bazy relacyjnej i zwracają najbardziej aktualną wersję danych).

System analityczny powinien udostępniać rozwiązania Data Mining (m.in. algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), podobieństw sekwencyjnych (Sequence Clustering), sieci neuronowych (Neural Nets) oraz Naive Bayes) oraz możliwość ich integracji ze strukturami wielowymiarowymi. Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.

System powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.

39. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators)

System powinien udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.

System powinien umożliwiać tworzenie takich wskaźników również w modelach danych wykorzystujących technologię in-memory BI.

40. Kreatory modelowania złożonych procesów biznesowych

System powinien udostępniać szereg łatwych w użyciu kreatorów pozwalających niezaawansowanym użytkownikom implementować złożone problemy analizy biznesowej w modelu analitycznym, czyniąc programowanie projektów BI przystępnym dla większej liczby osób i organizacji.

41. Aktywne buforowanie danych - Proactive caching

System powinien udostępniać mechanizm odświeżania danych w strukturach wielowymiarowych, który wykrywa zmiany w systemach źródłowych i na bieżąco aktualizuje bazę wielowymiarową.

42. System raportowania

System RBD powinien posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępniane przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki) bez konieczności stosowania dodatkowego oprogramowania po stronie serwera.

Dodatkowo system raportowania powinien obsługiwać:

- raporty parametryzowane
- *cache* raportów (generacja raportów bez dostępu do źródła danych)
- *cache* raportów parametryzowanych (generacja raportów bez dostępu do źródła danych z różnymi wartościami parametrów)
- współdzielenie predefiniowanych zapytań do źródeł danych
- wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File)
- możliwość opublikowania elementu raportu (wykresu, tabeli) do współdzielonej biblioteki, z której mogą korzystać inni użytkownicy, tworząc nowy raport ze znajdujących się w bibliotece elementów raportowych
- możliwość wizualizacji wskaźników KPI,
- możliwość wizualizacji danych w postaci obiektów sparkline

Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).

Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel (od wersji 1997 do 2010), Microsoft Word (od wersji 1997 do 2010), HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystywać jako źródło danych w innych aplikacjach.

System RBD powinien umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.

System RBD powinien umożliwiać wysyłkę raportów w wybranym formacie (drogą mailową) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).

System raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.

43. Narzędzia do tworzenia raportów ad-hoc

System powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez niezaawansowanych użytkowników. Tworzenie raportów powinno odbywać się w środowisku graficznym. Użytkownicy powinni mieć możliwość na publikowanie stworzonych raportów na serwerze w celu udostępnienia ich szerszemu gronu osób.

44. Zintegrowanie narzędzia do zarządzania systemem

System powinien dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych).

Narzędzia te powinny udostępniać możliwość tworzenia i wykonywania skryptów zarządzających RBD oraz silnikiem baz wielowymiarowych OLAP.

45. Możliwość tworzenia funkcji i procedur w innych językach programowania

System powinien umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego RBD. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.

46. Możliwość zarządzania centralnymi słownikami danych

System powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM).

System MDM powinien:

- udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach
- wersjonowanie danych (możliwość śledzenia zmian wprowadzonych przez użytkowników z możliwością ich cofnięcia do wybranej wersji)
- udostępniać mechanizm tworzenia i uruchamiania reguł walidujących poprawność danych w słownikach
- udostępniać narzędzia do administracji i kontroli uprawnień dostępu do danych w MDM
- udostępniać zestaw bibliotek (API programistyczne) z funkcjonalnościami MDM do wykorzystania w aplikacjach użytkownika
- umożliwiać eksport danych zgromadzonych w systemie MDM
- umożliwiać zarządzanie danymi podstawowymi z poziomu programu Microsoft Excel

47. Możliwość rejestrowania bardzo dużej liczby zdarzeń i analizowania ich z minimalnym opóźnieniem

System powinien dostarczać wbudowaną platformę do tworzenia aplikacji typu CEP (Complex Event Processing). Aplikacje takie umożliwiają rejestrowanie bardzo dużej liczby zdarzeń i reagowanie na nie z minimalnym opóźnieniem.

System powinien również udostępniać mechanizmy wysokiej dostępności dla tej usługi.

48. Narzędzia do zarządzania jakością danych

System powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji.

W ramach tych funkcji powinien:

- udostępniać funkcje do profilowania danych (analiza i raporty dot. jakości danych)
- udostępniać funkcje do deduplikacji danych
- określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną (którą może ale nie musi zaakceptować użytkownik)
- umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów)
- umożliwiać definiowanie złożonych domen (zestawu kilku atrybutów) oraz ocenę jakości danych na podstawie powiązań między tymi atrybutami (np. weryfikację poprawności danych adresowych złożonych z kodu pocztowego, miasta i ulicy)
- pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania)
- umożliwiać eksport wyników badania (poprawnych i sugerowanych wartości) do pliku tekstowego lub bazy relacyjnej; eksport powinien obejmować wartości po korekcie (poprawione) oraz ewentualnie te przed korektą (błędne)
- przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy)
- umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych
- zapewniać mechanizmy „uczenia się” bazy wiedzy – czyli w miarę realizacji kolejnych procesów ręcznego czyszczenia danych baza wiedzy powinna umożliwiać gromadzenie tych informacji na potrzeby kolejnych procesów
- umożliwiać wykorzystanie bazy wiedzy w automatycznym procesie czyszczenia danych (powinien integrować się z narzędziami do ekstrakcji, transformacji i ładowania danych, dzięki czemu będzie można wykorzystać te mechanizmy w automatycznym procesie ładowania danych)

1.13. Serwer zarządzania projektami

Serwer zarządzania projektami ma być oparty na platformie portalu wielofunkcyjnego i musi spełniać następujące wymagania:

1. Możliwość zarządzania projektami i portfelami projektów.
2. Natywne wykorzystanie środowiska portalu wielofunkcyjnego, jako interfejsu użytkownika.
3. Możliwość implementacji przyjętych w skali organizacji procedur zarządzania projektami. Planowanie, śledzenie i kontrola realizacji projektów muszą odbywać się w oparciu o procedury przyjęte w ramach własnych doświadczeń projektowych. Wymagana jest implementacja rozwiązania umożliwiającego śledzenie realizowanych projektów, postępów prac, obciążenia zasobów, kontrolę kosztów etc.
4. Dane dotyczące realizowanych projektów i dokumentacja projektowa muszą być przechowywane w sposób bezpieczny z gwarancją dostępu dla uprawnionych osób. System ma umożliwić dostęp do aktualnego statusu prowadzonych projektów.
5. Kontrola, rozpatrywanie i zatwierdzanie dokumentów za pomocą definiowalnego przepływu roboczego (workflow),
6. System zarządzania projektami:
 - a. szybki wgląd w aktualny status realizowanych projektów,
 - b. określenie kosztów ponoszonych w poszczególnych projektach,
 - c. ocenę prac w zakresie zgodności z harmonogramem i przyjętym budżetem,
 - d. określenie zasobów zaangażowanych w realizację poszczególnych projektów i poziomu ich zaangażowania,
 - e. określenie odpowiedzialności za realizację poszczególnych zadań i projektów,
 - f. aktualną ocenę stanu dostępności zasobów w organizacji.

Ze względu na to, że Zamawiający realizuje dużą liczbę równoczesnych projektów, a każdy kierownik projektu ma różne potrzeby, charakterystyczne dla pełnionych przez niego ról, wybrane rozwiązanie ma udostępniać poszczególnym grupom odbiorców różne cechy i funkcjonalność.

1. Zarządzanie projektami

System zarządzania projektami ma zapewnić sprawną koordynację i zarządzanie projektami. Dzięki Centralnemu Repozytorium Projektów (CRP), kierownictwo ma utrzymywać oraz wdrażać szablony planów projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.

Wymagane informacje o Projekcie

- a. Definiowanie inicjatyw projektowych,
- b. Definiowanie typów projektów dla wszystkich żądań i możliwość powiązania ich z cyklami pracy, planem projektu i zindywidualizowanymi szablonami miejsca pracy.
- c. Przygotowanie harmonogramów,
 - Opis listy zadań do wykonania
 - Określenie struktury hierarchicznej zadań (WBS)
 - Określenie zależności między zadaniami – relacje,
- d. Zapisywanie projektów do centralnego repozytorium,
- e. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
- f. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,
- g. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
- h. Przeglądanie informacji o projektach za pomocą przeglądarki internetowej,
- i. Grupowanie projektów według zadanych kryteriów,
 - Etap projektu,
 - Lokalizacja projektu,
 - Kierownik projektu,
 - Itp.

- j. Sygnalizacja graficzna opóźnień zadania względem planu bazowego
 - Informacja czy jest plan bazowy,
 - Informacja o odchyleniu względem czasu,
 - Informacja o odchyleniu względem kosztu,
 - Informacja o odchyleniach względem pracy,
- k. Śledzenie postępu realizacji projektu
 - Analiza czasu,
 - Analiza kosztu,
 - Analiza godzin przepracowanych,
- l. Raportowanie
 - Informacja o zadaniach opóźnionych,
 - Informacja o kosztach zadań,
 - Informacja o pracy w zadaniach,
- m. Delegowanie uprawnień do projektu,
- n. Zmiana właściciela projektu,
- o. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
- p. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów,

2. Zarządzanie portfelami projektów

System zarządzania projektami ma zapewnić sprawną koordynację i zarządzanie wszystkimi prowadzonymi projektami poprzez ustalenie zależności między projektami i używanymi do nich zasobami. W związku z tym system musi posiadać następujące cechy:

- a. Narzędzia pozwalające na wybór optymalnego portfela projektów dostosowany do różnych ograniczeń, w tym budżetowych.
- b. Analizy pozwalające określić priorytetowe projekty ze względu na wiele czynników – wartość strategiczną, wartość finansową i ryzyko.
- c. Narzędzia pozwalające porównywać scenariusze optymalizacji projektów za pomocą kart wyników.
- d. Narzędzia pozwalające na zmianę terminów projektów wewnątrz horyzontu czasowego planowania, w celu zoptymalizowania wykorzystania zasobów przy zachowaniu współzależności projektów.

1.14. Pakiet zarządzania projektami

Pakiet zarządzania projektami ma zapewnić możliwość wspomagania dla prowadzenia projektów, między innymi w zakresie tworzenia, oraz wdrażania szablonów planów projektów. Ma zapewnić rozwiązania umożliwiające elastyczne zarządzanie pracą oraz narzędzia do współpracy potrzebne kierownikom projektów. Wraz z rozwojem potrzeb ma umożliwić korzystanie z bardziej zaawansowanych narzędzi do zespołowego zarządzania projektami i portfelem projektów. Zarządzanie projektami ma zapewnić uzyskanie jednolitych raportów przedstawianych przełożonym oraz instytucjom zewnętrznym, w tym jednostkom prowadzącym audyty projektów.

Pakiet musi umożliwiać planowanie i udostępnianie wymaganych informacji o projekcie, takich jak:

- 1. Definiowanie projektów,
- 2. Przygotowanie harmonogramów,
 - a. Opis listy zadań do wykonania
 - b. Określenie struktury hierarchicznej zadań (WBS)
 - c. Określenie zależności między zadaniami – relacje,
- 3. Tworzenie planów bazowych
- 4. Zapisywanie projektów,
- 5. Przygotowanie szablonów harmonogramów i opublikowanie ich do repozytorium szablonów,
- 6. Automatyczne przekształcanie inicjatyw projektowych w projekty przy wykorzystaniu szablonów projektowych,

7. W zależności od wybranych kategorii dla inicjatywy projektowej, tworzony projekt powinien zawierać harmonogram charakterystyczny dla danego typu projektu,
8. Opcje automatycznego planowania terminów zadań, wyliczające daty i okresy trwania.
9. Wizualizacja osi czasu przedstawiającej harmonogram i plan projektu.
10. Wsparcie dla planowania kroczącego i tworzenia prognoz, wykorzystujących ręcznie wprowadzone do harmonogramu zadania sumaryczne Top Down.
11. Identyfikacja braków zasobów poprzez porównanie zaplanowanych ręcznie zadań sumarycznych z informacjami wpływającymi z podzadań.
12. Definicja aktywnych i nieaktywnych zadań, umożliwiająca przeprowadzenie analizy wielowariantowej.
13. Bilansowanie nadmiernie przydzielonych zasobów – zarówno automatycznie dla całego harmonogramu, jak i ręcznie dla poszczególnych zadań.
14. Grupowanie projektów według zadanych kryteriów,
 - a. Etap projektu,
 - b. Lokalizacja projektu,
 - c. Kierownik projektu,
 - d. Itp.
15. Sygnalizacja graficzna opóźnień zadania względem planu bazowego
 - a. Informacja czy jest plan bazowy,
 - b. Informacja o odchyleniu względem czasu,
 - c. Informacja o odchyleniu względem kosztu,
 - d. Informacja o odchyleniach względem pracy,
16. Śledzenie postępu realizacji projektu
 - a. Analiza czasu,
 - b. Analiza kosztu,
 - c. Analiza godzin przepracowanych,
17. Zmiana właściciela projektu,
18. Dynamiczna zmiana właściciela projektu, zgodnie z wyborem kierownika projektu,
19. Kontrola zmian pól opisujących projekt – zmianę pól może dokonywać tylko administrator lub biuro projektów.
20. Łatwą analizę danych poprzez definiowanie filtrów dla kolumn.
21. Szeroki zakres formatowania tekstu.
22. Natywna integracja z składnikami pakietu biurowego między innymi poprzez możliwość przenoszenia informacji do aplikacji pakietu biurowego przy zachowaniu formatowania dzięki funkcjom kopiowania i wklejania.
23. Integracja ze środowiskiem serwerowym Microsoft Project Server 2010 – pełna, dwukierunkowa synchronizacja danych.
24. Możliwość przypisywania zasobów z Active Directory.
25. Pakiet musi zawierać licencję dostępową do serwera zarządzania projektami.

1.15. Licencje dostępowe do serwera zarządzania projektami

Licencje dostępowe umożliwiające użytkownikom wykorzystanie funkcjonalności serwera zarządzania projektami.

1.16. Zintegrowane środowisko programistyczne

Zintegrowane środowisko programistyczne powinno bez stosowania dodatkowego oprogramowania:

1. Umożliwiać tworzenie aplikacji dla Windows, aplikacji internetowych, aplikacji opartych na Microsoft Office system, platformie .NET Framework, SQL Server, Windows Azure za pomocą zintegrowanych kreatorów obsługiwanych metodą przeciągnij i upuść,
2. Umożliwiać zintegrowaną obsługę języków Visual Basic, Visual C# i Visual C++ , która pozwala na stosowanie różnych stylów programowania,

3. Obsługiwać funkcje edytora, takie jak zmień i kontynuuj, które upraszczają cykl projektowania, tworzenia kodu i debugowania aplikacji,
4. Obsługiwać wdrażanie aplikacji klienckich z wykorzystaniem ClickOnce, dzięki której programiści i specjaliści IT mogą wdrażać aplikacje i wymagane przez nie komponenty w sposób gwarantujący stałą aktualność aplikacji,
5. Obsługiwać tworzenie aplikacji opartych na .NET Framework, pozwalające na skrócenie czasu opracowywania aplikacji ze względu na mniejszą ilość niezbędnego kodu infrastrukturalnego i podniesienie bezpieczeństwa aplikacji,
6. Wykorzystywać ASP.NET do przyspieszenia tworzenia interaktywnych, atrakcyjnych aplikacji internetowych oraz usług sieciowych. Strony wzorcowe (master pages) umożliwiają utworzenie spójnego wyglądu witryny i zarządzanie wyglądem wielu stron z jednego miejsca
7. Umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet
8. Umożliwiać pobieranie darmowych aktualizacji w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bezpłatnie) – wymagane podanie nazwy strony www
9. Posiadać graficzny interfejs użytkownika
10. Posiadać zintegrowane graficzne narzędzie do projektowania interfejsu użytkownika
11. Posiadać zintegrowane funkcjonalności umożliwiające współdzielenie zadań i zarządzanie projektem
12. Posiadać zintegrowane narzędzia do automatyzacji i nagrywania testów webowych
13. Umożliwiać generowanie i uruchamianie testów obciążeniowych
14. Posiadać narzędzia do refaktoringu bazy danych
15. Posiadać narzędzia do kontroli jakości kodu
16. Umożliwiać monitorowanie wskaźników wydajności serwera podczas testów obciążeniowych
17. Posiadać zorganizowany system szkoleń i materiały edukacyjne w języku polskim
18. Umożliwiać dokonywanie zmian kodu podczas sesji debugowania na platformie x86
19. Zawierać szablony projektowe dostosowane do MSF Agile i MSF CMMI
20. Umożliwiać bezpieczną pracę zdalną i lokalną z repozytorium kodu źródłowego
21. Wspierać z zintegrowanym środowiskiem pracę z zadaniami, zapewniać mechanizmy powiązania zadań z kodem oddawanym przez programistów
22. Zapewniać mechanizmy automatycznej kompilacji rozwiązań .Net oraz automatycznie uruchamiać testy jednostkowe i generować raporty pokazujące listę błędów
23. Możliwość tworzenia testów jednostkowych interfejsu użytkownika poprzez nagrywanie interakcji użytkownika z aplikacją.
24. Posiadać narzędzia pozwalające na tworzenie rozwiązań dla SharePoint Portal Server
25. Posiadać możliwość budowania rozwiązań Silverlight
26. Wspierać tworzenie diagramów UML
27. Mieć możliwość nagrywania stanu aplikacji w celu historycznego debugowania aplikacji.

1.17. Pakiet usług wsparcia technicznego do posiadanego i zamawianego oprogramowania

Pakiet usług musi obejmować swoim zakresem świadczenie opieki serwisowej do posiadanego i zamawianego oprogramowania w okresie **36 miesięcy** od daty podpisania przez Zamawiającego Protokołu Odbioru Licencji.

W wymaganiach zastosowano następujące definicje:

1. Podstawowe Godziny Wsparcia – dni robocze od godz. 09:00 do godz. 17:00, czasu środkowoeuropejskiego.
2. Pozostałe Godziny Wsparcia – dni robocze od godz. 17:00 do godz. 09:00 dnia następnego, niedziele i święta określone w przepisach o dniach wolnych od pracy.
3. Czas Reakcji – maksymalny czas pomiędzy zgłoszeniem problemu, a przystąpieniem do analizy Problemu i poszukiwaniu rozwiązania.
4. Czas Reakcji „on-site” – czas pomiędzy potwierdzeniem przyjęcia zgłoszenia a pojawieniem się Inżyniera Wsparcia na miejscu w siedzibie Zamawiającego.

5. Waga Problemu – miara ważności Problemu ustalana przez Zamawiającego:

- a. Problem **krytyczny** - mający krytyczny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe krytyczne dla działalności biznesowej Zamawiającego przestały funkcjonować i potrzebna jest natychmiastowa pomoc.
- b. Problem **poważny** - mający poważny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują w sposób poważnie utrudniający normalną pracę lub nie funkcjonują w ogóle – potrzebna jest pomoc nie później niż w czasie 1 godziny od zgłoszenia problemu.
- c. Problem **umiarkowany** - mający umiarkowany wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują w sposób utrudniający normalną pracę – potrzebna jest pomoc nie później niż w czasie 2 godzin od zgłoszenia problemu.
- d. Problem **minimalny** - mający minimalny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują poprawnie, aczkolwiek występują pewne drugorzędne i prawie niezauważalne trudności – potrzebna jest pomoc ze nie później niż w czasie 4 godzin od zgłoszenia Problemu.

Dla problemów umiarkowanych i minimalnych w okresie tzw. Pozostałych Godzin Wsparcia nie jest wymagany ustalony czas reakcji.

Wymagane jest zapewnienie opieki serwisowej nad dostarczonym oprogramowaniem na następujących zasadach:

1. Wykonawca będzie świadczyć usługi w zakresie organizacji i koordynacji usług w zakresie wsparcia technicznego oprogramowania wyprodukowanego przez producenta oprogramowania lub spółki zależne producenta (Producenta), w odniesieniu do którego nie zakończył się tzw. okres dodatkowego wsparcia.
2. Wsparcie dotyczyć będzie oprogramowania posiadanego przez Zamawiającego, będącego przedmiotem niniejszego postępowania (Produktów).
3. Usługi w zakresie wsparcia technicznego będą świadczone przez okres **36 miesięcy** od daty podpisania przez Zamawiającego Strony Protokołu Odbioru Licencji.
4. Wykonawca zapewni możliwość bezpośredniego zgłaszania problemów technicznych do producenta oprogramowania lub spółki zależnej producenta (Producenta) drogą elektroniczną poprzez dedykowaną stronę producenta i telefonicznie.
5. Wykonawca zagwarantuje możliwość wykonywania poprawek do oprogramowania (HotFix) przez Producenta.
6. Warunki świadczenia usług w zakresie wsparcia technicznego Produktów:
 - a. Usługi w zakresie wsparcia technicznego (Produktów) mają obejmować:
 - Usługi reaktywne, czyli świadczenie Zamawiającemu przez certyfikowanych specjalistów, pracowników Producenta, pomocy przy rozwiązywaniu problemów dotyczących Produktów, które pojawiły się u Zamawiającego przy korzystaniu z takich Produktów, jeżeli zachodzi uzasadnione podejrzenie, że taki problem został spowodowany przez Produkty (w szczególności, z możliwością tworzenia poprawek z wykorzystaniem dostępu do kodu źródłowego Produktów).
 - Usługi proaktywne, czyli usługi mające na celu efektywne i skuteczne zapobieganie problemom dotyczącym Produktów polegające w szczególności na okresowych spotkaniach z certyfikowanymi specjalistami Producenta Produktów i przygotowywaniu odpowiednich raportów, uzyskaniu dostępu do poprawek do Produktów czy zasobów Producenta z artykułami i wskazówkami dotyczącymi rozwiązywania i zapobiegania Problemom.
 - b. Zamawiający ma uzyskać priorytetowy dostęp, przez zapewnienie dedykowanego numeru telefonicznego i internetowego dostępu technicznego do certyfikowanych specjalistów Producenta w celu szybkiego zgłaszania problemów dotyczących Produktów oraz uzyskiwania wsparcia.
 - c. W ramach usług wsparcia technicznego Zamawiający wymaga przedstawienia oferty na standardowe pakiety wsparcia technicznego zawierające:
 - Nie mniej niż 480 godzin roboczych działań proaktywnych (do 160 godzin rocznie) – związanych z zapobieganiem problemom,

- Nie mniej niż 420 godzin roboczych reaktywnych (do 140 godzin rocznie) – związanych z rozwiązywaniem zgłoszonych problemów technicznych możliwych do wykorzystania w okresie trwania umowy.

W przypadku, gdy godziny reaktywne nie byłyby wykorzystane, musi istnieć możliwość konwersji ich na godziny usług proaktywnych.

- d. Zamawiający wymaga możliwości konwersji niewykorzystanych godzin przeznaczonych na działania proaktywne do godzin przeznaczonych na działania reaktywne.
- e. Wymagane jest umożliwienie wsparcia technicznego dla Produktów wychodzących z okresu tzw. wsparcia rozszerzonego, to znaczy dla Produktów, które na podstawie innych umów nie są objęte wsparciem Producenta.
- f. Usługi w zakresie wsparcia technicznego Produktów powinny być dostępne przez 24 godziny na dobę i 7 dni w tygodniu. Zgłoszenia problemów będą dokonywane bezpośrednio do Producenta na dedykowany numer telefoniczny (dla wszystkich zgłoszeń) lub zgłaszane w formie elektronicznej na dedykowanym serwisie internetowym (dla zgłoszeń umiarkowanych i minimalnych), do certyfikowanych specjalistów Producenta. Termin rozpoczęcia prac nad zgłoszonym problemem objętym usługami w zakresie wsparcia technicznego Produktów przez takich specjalistów (tzw. czas reakcji) powinien zależeć od wagi zgłaszanego problemu:
 - Problemy **krytyczne i poważne** - czas reakcji telefonicznej do jednej godziny w trybie 24 godziny na dobę i 7 dni w tygodniu;
 - Problemy **umiarkowane** - czas reakcji 2 godziny w godzinach 9-17 od poniedziałku do piątku z wyłączeniem, świąt i dni wolnych od pracy na podstawie przepisów prawa;
 - Problemy **minimalne** - czas reakcji 4 godziny w godzinach 9-17 od poniedziałku do piątku z wyłączeniem, świąt i dni wolnych od pracy na podstawie przepisów prawa.
- g. W ramach usług w zakresie wsparcia technicznego Produktów będzie istniała możliwość świadczenia takich usług na miejscu w lokalizacji Zamawiającego (tzw. usługi wsparcia „on-site”). Usługi świadczone w lokalizacji Zamawiającego w Polsce będą rozliczane w ramach dostępnej dla Zamawiającego puli godzin usług, o których mowa w pkt. 1.17 6 c powyżej. Lista lokalizacji zamawiającego stanowi załącznik do specyfikacji.
- h. Wykonawca zapewni regularne przekazywanie Zamawiającemu przez Producenta informacji technicznych w postaci biuletynu technicznego osobom kontaktowym wskazanym przez Zamawiającego.
- i. W ramach usług w zakresie usług wsparcia technicznego do Zamawiającego zostanie przypisany dedykowany specjalista Producenta, który będzie odpowiedzialny za realizację usług w zakresie wsparcia technicznego dla Zamawiającego, a także za przekazywanie oraz otrzymywanie informacji i komentarzy zwrotnych dotyczących świadczonych usług. Jednocześnie Zamawiający w terminie do 14 dni od daty podpisania Umowy wyznaczy ze swojej Strony osoby (w tym koordynatora wsparcia technicznego) uprawnione do składania u specjalisty Producenta zgłoszeń w ramach usług w zakresie wsparcia technicznego Produktów.
- j. Po podpisaniu umowy w zakresie usług wsparcia technicznego, w uzgodnionym terminie, przedstawiciel Producenta przeprowadzi sesję orientacyjno-przeglądową u Zamawiającego. Sesja może być przeprowadzona telefonicznie lub w lokalizacji Zamawiającego. Celem takiej sesji jest szczegółowe omówienie dostępnych usług w zakresie wsparcia technicznego, zasad ich świadczenia, zebranie informacji o potrzebach Zamawiającego w zakresie wsparcia oraz opracowanie planu współpracy obejmującego okres świadczenia usług wsparcia technicznego, który będzie dokumentem roboczym, przeglądany i uaktualniany przez strony w regularnych odstępach czasu i który będzie obejmował wiedzę na temat planowanych i aktualnych działań w stosunku do Zamawiającego, jak również usług wykonanych w przeszłości.

1.18. Usługi stowarzyszone

W ramach przedmiotu Zamówienia Zamawiający wymaga:

- a) Wszystkie osoby wyznaczone przez wykonawcę do procesów wdrażania usługi, mają posiadać ważne certyfikaty producenta z zakresu instalacji powierzonego im do instalacji oprogramowania

b) Wdrożenia ze względu na bezpieczeństwo obecnie pracującego systemu produkcyjnego ma być przeprowadzone w następujących fazach

Ip	Nazwa	Godz.	Czas trwania (tygodnie)	Role
1	Wdrożenie usługi katalogowej i system poczty elektronicznej	940	15	
1.1	Faza wizji i zakresu. Produkty: <i>Dokument wizji i zakresu,</i> <i>Wysoko poziomowy plan projektu</i> <i>Dokument z wymaganiami</i>	80	2	Architekt; Project Manager; Konsultant
1.2	Planowanie Produkty: <i>Specyfikacja Funkcjonalna,</i> <i>Plan Projektu</i>	140	2	Architekt; Project Manager; Konsultant
1.3	Budowa rozwiązania Produkty: <i>Dokumentacja Wdrożeniowa (Budowa środowiska, Migracja), Dokumentacja DR;</i> <i>Plan testów</i>	320	4	Architekt; Project Manager; Konsultant
1.4	Stabilizacja Produkty: <i>Wyniki Testów</i>	80	2	Architekt; Project Manager; Konsultant
1.5	Wdrożenie Produkty: <i>Procedury operacyjne,</i> <i>Zainstalowane serwery,</i> <i>Zmigrowani użytkownicy</i>	320	5	Architekt; Project Manager; Konsultant

c) W zakresie usług wymagane jest zapewnienie:

1. Wykonanie usług przez specjalistów (pracowników).
2. Dostęp do laboratoriów i specjalistów Producenta, który pozwoli na:
 - (a) możliwość testowania specyficznych scenariuszy rozwiązań klienta w laboratorium Producenta,
 - (b) możliwość szybkiego rozwiązywania problemów w ramach wsparcia projektów wdrożeniowych, poprzez przygotowanie dedykowanych dla danej sytuacji poprawek w kodzie (tzw. HOT FIXy).
3. Dostęp do bazy wiedzy Produktów,
 - (a) Dostęp do bazy wiedzy Producenta oraz do zastrzeżonych prawami autorskimi bibliotek architektur referencyjnych i najlepszych praktyk w obszarze wdrożenia i eksploatacji produktów Producenta.
 - (b) Dostęp do historii wszystkich incydentów (awarii) dotyczących produktów Producenta i rozwiązań, zgłoszonych przez klientów Producenta na całym świecie.
4. Zapewnienie informacji o nowych wersjach i funkcjonalnościach produktów przed oficjalnym upublicznieniem:
 - (a) informacja o datach dostępności i datach planowanego zakończenia wsparcia,
 - (b) możliwości otrzymania wersji przedprodukcyjnych w tym wersji Beta do testów, uczestnictwo w programach *Technology Adoption Program* – (TAP) po przejściu procesu kwalifikacyjnego)
5. Możliwość zgłaszania wymagań do grup produktowych Producenta

Waga Problemu	Podstawowe godziny wsparcia		Pozostałe godziny wsparcia	
	Czas reakcji	Zobowiązania WYKONAWCY	Czas reakcji	Zobowiązania WYKONAWCY
1	1h	Pracownik WYKONAWCY udaje się do siedziby ZAMAWIAJĄCEGO tak szybko jak jest to możliwe. Problem jest szybko eskalowany wewnątrz Wykonawcy do zespołów produktowych O zaistniałej sytuacji powiadamiane jest kierownictwo Wykonawcy Prace nad zgłoszonym Problemem	1h	Pracownik WYKONAWCY udaje się do siedziby ZAMAWIAJĄCEGO tak szybko jak jest to możliwe. Problem jest szybko eskalowany wewnątrz Wykonawcy do zespołów produktowych O zaistniałej sytuacji powiadamiane jest kierownictwo Wykonawcy Prace nad zgłoszonym

				Problemem prowadzone są w systemie 24*7
A	1h	O zaistniałej sytuacji powiadamiane jest kierownictwo Wykonawcy Prace nad zgłoszonym Problemem prowadzone są w systemie 24*7	1h	O zaistniałej sytuacji powiadamiane jest kierownictwo Wykonawcy Prace nad zgłoszonym Problemem prowadzone są w systemie 24*7
B	2h	Prace nad zgłoszonym Problemem prowadzone są tylko w Podstawowych Godzinach Pracy	Nie dotyczy	
C	4h	Prace nad zgłoszonym Problemem prowadzone są tylko w Podstawowych Godzinach Pracy	Nie dotyczy	

Tab. 1 Czasy reakcji

Podstawowe godziny wsparcia są rozumiane jako: Dni robocze od godz. 09:00 do godz. 17:00, czasu środkowoeuropejskiego.

Pozostałe godziny wsparcia są rozumiane jako godziny nie wchodzące w skład podstawowych godzin wsparcia.

Tab. 2 Wagi problemu

Waga problemu	Definicja wagi
1	Problem krytyczny - mający krytyczny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe krytyczne dla działalności biznesowej Zamawiającego przestały funkcjonować i potrzebna jest natychmiastowa pomoc.
A	Problem poważny - mający poważny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują w sposób poważnie utrudniający normalną pracę lub nie funkcjonują w ogóle – potrzebna jest pomoc nie później niż w czasie 1 godziny od zgłoszenia problemu.
B	Problem umiarkowany - mający umiarkowany wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują w sposób utrudniający normalną pracę – potrzebna jest pomoc nie później niż w czasie 2 godzin od zgłoszenia problemu.
C	Problem minimalny - mający minimalny wpływ na procesy biznesowe Zamawiającego. Procesy biznesowe Zamawiającego funkcjonują poprawnie, aczkolwiek występują pewne drugorzędne i prawie niezauważalne trudności – potrzebna jest pomoc ze nie później niż w czasie 4 godzin od zgłoszenia Problemu.

Wykonawca zobowiązuje się do świadczenia pomocy technicznej zgodnie z wytycznymi z Tab. 1 oraz Tab 2. przy czym:

- Czas reakcji rozumiany jest jako czas od momentu przyjęcia zgłoszenia do momentu podjęcia działań.
- Zgłoszenie rozumiane jest jako kontakt pracownika firmy Zamawiającego z pracownikiem Wykonawcy:
- Telefonicznie na numer
- Za pośrednictwem poczty elektronicznej na adres
- Bądź przy użyciu specjalnej strony internetowej o adresie

Zamawiający dopuszcza przelanie zobowiązań niniejszego SLA z Wykonawcy na Producenta zamawianego oprogramowania.

Powyższe zapisy dotyczące gwarancji określają odpowiedzialność Wykonawcy za wady w sposób pełny.

Po upływie okresu gwarancyjnego Wykonawca może ewentualnie świadczyć usługi serwisowe utrzymania w sprawności oprogramowania będącego Przedmiotem Umowy, na warunkach i w sposób określony w oddzielnej umowie serwisowej.