Załącznik Nr 1 do SIWZ

Spis treści

Część „A”

1. Wymagania w zakresie dostaw

Przedmiotem zamówienia jest dostawa pakietów subskrypcji oprogramowania standardowego oraz oprogramowania z licencjami z prawem do aktualizacji (dalej łącznie nazywanych Produktami) w ramach 36-cio miesięcznej umowy.

Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).

Zamawiający wymaga dostawy Produktów na warunkach przewidzianych przez producenta Produktów (Producenta) dla jednostek Skarbu Państwa.

W związku z faktem, iż Zamawiający przewiduje prawo opcji w niniejszym zamówieniu, Zamawiający gwarantuje dokonanie zakupu w ramach zamówienia podstawowego Produktów w liczbie określonej w kolumnie „liczba Produktów gwarantowanych” i przewiduje, w ramach prawa opcji, możliwość zakupu Produktów wymienionych w kolumnach „liczba Produktów opcjonalnych” w pierwszym, drugim lub trzecim roku trwania umowy.

Specyfikacja ilościowa przedmiotu zamówienia:

Lp.	Typ oprogramowania	Liczba produktów gwarantowanych	Liczba produktów opcjonalnych
1	Subskrypcja usług komunikacyjnych, bezpieczeństwa i oprogramowania klasy desktop (subskrypcja na użytkownika)	4000	1500
2	Serwerowy system operacyjny z elementami zarządzania z prawem do aktualizacji typ I (licencja na 2 rdzenie procesora)	632	64
3	Serwerowy system operacyjny z elementami zarządzania z prawem do aktualizacji typ II (licencja na 2 rdzenie procesora)	112	32
4	Serwer relacyjnej bazy danych z prawem do aktualizacji (licencja na 2 rdzenie procesora)	24	12
5	Subskrypcja pakietu zarządzania projektami	5	5
6	Subskrypcja pakietu modelowania graficznego	5	5
7	Pakiet usług wsparcia technicznego	1	0

Tabela 1 – specyfikacja ilościowa zamawianych produktów.

1.1. Wymagania ogólne w zakresie dostaw

1. Zamawiający wymaga zagwarantowania niezmienności cen Producenta na Produkty w całym okresie trwania umowy, z wyłączeniem zmian kursowych EUR/PLN.
2. Oprogramowanie musi pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu).
3. Oferowane subskrypcje usług hostowanych muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i normatywów potwierdzonych aktualnymi wynikami niezależnych audytów, w szczególności:
    a) ISO 27001, ISO 27002, ISO 27017, ISO 27018
    b) UK G-Cloud
    c) SOC 1, SOC 2
    d) Open Authentication Standard – OAuth

4. Oprogramowanie i subskrypcje oprogramowania muszą gwarantować prawo instalacji najnowszej wersji oprogramowania dostępnej w trakcie trwania umowy.
5. Oprogramowanie musi pozwalać na udzielenie licencji oprogramowania dla jednostek stowarzyszonych.
6. Zamawiający dopuszcza oferowanie Produktów o szerszej niż opisana funkcjonalności.
7. 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 Produkty, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej.
8. W związku z możliwością zwiększenia liczby użytkowników systemów w trakcie trwania umowy, Zamawiający wymaga zaoferowania licencjonowania gwarantowanego przez Producenta Produktów, umożliwiającego w okresie trwania umowy instalację dodatkowych licencji z zamawianego zakresu Produktów z możliwością rozliczania się za nie post factum - raz do roku.
9. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:
   a. Pobieranie zakupionego oprogramowania,
   b. Aktywację zakupionego oprogramowania,
   c. Sprawdzanie liczby zakupionych Produktów w wykazie zakupionych Produktów.
10. Zamawiający wymaga udzielenia uprawnień na stronie Producenta w terminie do 10 dni roboczych od podpisania umowy.
11. Po dziewięćdziesięciu (90) dniach od zakończenia okresu trwania umowy Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Producenta i usunięcie jego danych.
12. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
13. Jeżeli nowa wersja Produktu zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego Produktu przez Zamawiającego.

2. Specyfikacja techniczno – eksploatacyjna i cech użytkowych oprogramowania.

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

Z uwagi na to, że ustawa 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. Sprawdzenie to, będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego z dołączeniem do usługi katalogowej Zamawiającego – Active Directory.

W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby zamawiającego w terminie 2 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu dostawy. W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy. Nieprzedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.

Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone oferentowi.

2.1. Subskrypcja usług komunikacyjnych, bezpieczeństwa i oprogramowania klasy desktop (subskrypcja na użytkownika)

2.1.1. Subskrypcja usług komunikacyjnych, bezpieczeństwa i oprogramowania klasy desktop (subskrypcja na użytkownika)

Subskrypcja pakietów usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego musi zawierać następujące oprogramowanie i usługi:

System operacyjny klasy desktop

System operacyjny klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Interfejs graficzny użytkownika pozwalający na obsługę:
    a. Klasyczną przy pomocy klawiatury i myszy,
    b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim,
3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
5. Wbudowany system pomocy w języku polskim;
6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne,
10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,

17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
22. Obsługa standardu NFC (near field communication),
23. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
24. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
25. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
26. Mechanizmy uwierzytelniania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
    d. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być zgodny ze specyfikacją FIDO.
27. Mechanizmy wieloskładnikowego uwierzytelniania.
28. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
29. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
30. Wsparcie dla algorytmów Suite B (RFC 4869)
31. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
32. 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
33. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
34. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
35. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
36. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
37. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
38. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
39. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
40. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
41. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,

42. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
43. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
44. 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,
45. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
46. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
47. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
48. Udostępnianie wbudowanego modemu,
49. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
50. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
51. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
52. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
53. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
54. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
55. Wbudowane w 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.
56. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
57. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
58. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
59. Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
60. Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
61. 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.
62. 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.
63. Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.

64. Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
65. Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
66. Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
67. Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów
68. Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
69. Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
70. Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
71. Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
72. 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
73. Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
74. Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
75. Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
76. Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
77. Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
78. Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
79. Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
80. Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
81. Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
82. Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.

Subskrypcja usługi hostowanej i pakietu biurowego

Subskrypcja powszechnie dostępnej, standardowej usługi hostowanej (on-line) typu COTS (Commercial Of-The-Shelf) ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi katalogowej typu LDAP, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Ponadto musi zawierać subskrypcję pakietu biurowego. Wymagania dotyczące usługi hostowanej:

1. Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę katalogową.
2. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3. Możliwość dodawania własnych nazw domenowych do usługi katalogowej.
4. Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.

5. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
6. W okresie obowiązywania subskrypcji Usługa będzie przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, w przypadku podjęcia decyzji o braku jej kontynuacji, Usługa będzie przechowywać dane Zamawiającego, które zostały w niej zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją Usługi zostanie wyłączone a dane Zamawiającego zostaną usunięte.
7. Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
8. Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
9. Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
10. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.
11. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
12. Usługa musi odpowiadać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych.
13. Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
14. Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania:

1. Usługa musi umożliwiać:
   a. obsługę poczty elektronicznej,
   b. zarządzanie czasem,
   c. zarządzania zasobami
   d. zarządzanie kontaktami i komunikacją.
2. Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:
   a. Zarządzania użytkownikami poczty,
   b. Wsparcia migracji z innych systemów poczty,
   c. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
   d. Wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty.
3. Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
   a. Posiadanego oprogramowania Outlook (2010, 2013 i 2016),
   b. Przeglądarki (Web Access),
   c. Urządzeń mobilnych.

Wymagane cechy usługi to:

- Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 40 GB,
- Standardowy i łatwy sposób obsługi poczty elektronicznej,
- Obsługa najnowszych funkcji Outlook 2013 i 2016, w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
- Współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
- Bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich:

1. Funkcjonalność podstawowa:
   - Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
   - Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
   - Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
   - Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia
   - Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.
2. Funkcjonalność wspierająca pracę grupową:
   - Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości
   - Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu
   - Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze
   - Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone
   - Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania
   - Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań
   - Obsługa list i grup dystrybucyjnych.
   - Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej i wiadomości błyskawicznych.
   - Możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu.
   - Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności.
   - Widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami.
   - Funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności.
   - Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego.
   - Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej.
   - Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów
   - Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.
3. Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
   - Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja
   - Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.

- 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.
- Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne.
- Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów.
- 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.
- 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.
- Odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS.
- Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji.
- Możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.

4. Wsparcie dla użytkowników mobilnych:
   - 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
   - Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.)
   - Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone
   - 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
   - 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.
   - Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

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

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

8. Wersjonowanie dokumentów (dla wersji roboczych),
9. Organizację pracy grupowej,
10. Wyszukiwanie treści,
11. Dostęp do danych w relacyjnych bazach danych,
12. Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13. Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio jako wbudowane właściwości produktu:

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. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0
   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 dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).
2. Projektowanie stron
   a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron,
   b. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML,
   c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP,
   d. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3. 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 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. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

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

Pakiet biurowy on-line musi spełniać następujące wymagania:

1. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika,

   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych
2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
   a. posiada kompletny i publicznie dostępny opis formatu,
   b. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
3. Pakiet biurowy on-line musi zawierać:
   a. Edytor tekstów
   b. Arkusz kalkulacyjny
   c. Narzędzie do przygotowywania i prowadzenia prezentacji
   d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
4. Edytor tekstów musi umożliwiać:
   a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
   b. Wstawianie oraz formatowanie tabel
   c. Wstawianie oraz formatowanie obiektów graficznych
   d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego
   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. Określenie układu strony (pionowa/pozioma)
   k. Wydruk dokumentów
   l. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010 i 2016z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu
   m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
5. Arkusz kalkulacyjny musi umożliwiać:
   a. Tworzenie raportów tabelarycznych
   b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d. Wyszukiwanie i zamianę danych
   e. Wykonywanie analiz danych przy użyciu formatowania warunkowego
   f. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   g. Formatowanie czasu, daty i wartości finansowych z polskim formatem
   h. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   i. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
   j. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
6. 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 2010, 2013 i 2016.

Usługa serwera komunikacji wielokanałowej on-line (SKW) wspomagająca wewnętrzną i zewnętrzną komunikację ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy:

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

W połączeniu z funkcjami aplikacji klienckich usługa ma zapewnić uprawnionym użytkownikom:

1. Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.
2. Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub internet.
3. Możliwość oceny jakości komunikacji głosowej i wideo.
4. Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5. Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.
6. Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7. Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.
8. Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9. Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10. Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.
11. Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12. Możliwość nagrywania telekonferencji przez uczestników.
13. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.

14. Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15. Wbudowane funkcjonalności: SIP Proxy.
16. Wbudowana funkcjonalność mostka konferencyjnego MCU.
17. Obsługa standardów: CSTA, TLS, SIP over TCP.
18. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
19. Kodowanie video H.264,
20. Wsparcie dla adresacji IPv4 i IPv6,
21. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
22. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników,
23. Możliwość szyfrowania połączeń.
24. Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
    a. Dołączania do telekonferencji,
    b. Szczegółowej listy uczestników
    c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu.
    d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli.
    e. Dostępu do udostępnianych plików,
    f. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
25. Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:
    a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
    b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
    c. Wsparcia telekonferencji:
        - Dołączania do telekonferencji,
        - Szczegółowej listy uczestników,
        - Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
        - Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
        - Głosowania,
        - Udostępniania plików i pulpitów,
        - Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
    b. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
    c. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.

Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów:

1. Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2. Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3. Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:

a. Uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
b. Dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
c. Możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

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

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

Subskrypcja pakietu biurowego

Usługa hostowana on-line musi zawierać subskrypcję pakietu biurowego spełniającego następujące wymagania:

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

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
2. Wymagania odnośnie interfejsu użytkownika:
   a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
   b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
   c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3. Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
4. Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
   a. posiada kompletny i publicznie dostępny opis formatu,
   b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),
   c. umożliwia kreowanie plików w formacie XML,
   d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
6. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.

8. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    a. Edytor tekstów
    b. Arkusz kalkulacyjny
    c. Narzędzie do przygotowywania i prowadzenia prezentacji
    d. Narzędzie do tworzenia drukowanych materiałów informacyjnych
    e. Narzędzie do tworzenia i pracy z lokalną bazą danych
    f. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
    g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
    h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
11. Edytor tekstów musi umożliwiać:
    a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
    c. Wstawianie oraz formatowanie tabel.
    d. Wstawianie oraz formatowanie obiektów graficznych.
    e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
    f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
    g. Automatyczne tworzenie spisów treści.
    h. Formatowanie nagłówków i stopek stron.
    i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
    j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
    k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
    l. Określenie układu strony (pionowa/pozioma).
    m. Wydruk dokumentów.
    n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
    o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007, Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
    p. Zapis i edycję plików w formacie PDF.
    q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
    r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,
    s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.
12. Arkusz kalkulacyjny musi umożliwiać:
    a. Tworzenie raportów tabelarycznych
    b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
    c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.

d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
g. Wyszukiwanie i zamianę danych
h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
i. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS
j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
l. Formatowanie czasu, daty i wartości finansowych z polskim formatem
m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).
p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

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

i. Wydruk publikacji.
j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

15. Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
a. Tworzenie bazy danych przez zdefiniowanie:
b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
c. Relacji pomiędzy tabelami
d. Formularzy do wprowadzania i edycji danych
e. Raportów
f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.

16. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,
b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
f. Automatyczne grupowanie poczty o tym samym tytule,
g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
j. Zarządzanie kalendarzem,
k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
l. Przeglądanie kalendarza innych użytkowników,
m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
n. Zarządzanie listą zadań,
o. Zlecanie zadań innym użytkownikom,
p. Zarządzanie listą kontaktów,
q. Udostępnianie listy kontaktów innym użytkownikom,
r. Przeglądanie listy kontaktów innych użytkowników,
s. Możliwość przesyłania kontaktów innym użytkowników,
t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

17. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
a. Pełna polska wersja językowa interfejsu użytkownika.
b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX 10 lub wyższych,
d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu

operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
g. Obsługa telekonferencji SKW:
    i. Dołączania do telekonferencji,
    ii. Szczegółowej listy uczestników,
    iii. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
    iv. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
    v. Głosowania,
    vi. Udostępniania plików i pulpitów,
    vii. Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
h. Możliwość zmiany kanału komunikacji z pośrednictwem wiadomości błyskawicznych do połączenia głosowego i/lub wideo w ramach pojedynczej, otwartej w aplikacji sesji (bez konieczności przełączania się pomiędzy aplikacjami).
i. Lista adresowa wraz ze statusem obecności, opisem użytkowników SKW, zdjęciami użytkowników, listą dostępnych do komunikacji z nimi kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji oraz wydzielania grup kontaktów typu ulubione lub ostatnie.
j. Status obecności, dający możliwość ręcznego ustawiania statusu (dostępny, zajęty, nie przeszkadzać, z dala od komputera, niedostępny), automatycznej synchronizacji z jego aktywnością w systemie operacyjnym stacji roboczej, a w przypadku instalacji wybranych systemów poczty elektronicznej – dostępu do informacji o dostępności użytkownika na bazie wpisów do jego kalendarza.
k. Możliwość rozszerzania listy adresowej o zewnętrznych użytkowników wraz z informacjami opisowymi i kontaktowymi,
l. Historia ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
m. Integracja ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
n. Definiowanie i konfiguracja urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników

Subskrypcja pakietu usług zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:

Wymagania ogólne

1. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,
2. Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),

3. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018,
4. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
5. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,
6. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
7. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
8. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
9. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
10. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
11. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
13. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
14. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
15. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej.
16. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
17. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
18. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
19. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

Wymagania funkcjonalne

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

Wymagane scenariusze użycia:

1. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej.

2. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,
3. Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
4. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
5. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur),
6. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:
System zarządzania tożsamością elektroniczną ma zapewniać pobieranie, agregację oraz synchronizacje danych o użytkownikach z różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego centrum certyfikacji (CA).
Bezpieczeństwo

- System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
- System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami *firewall* oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
- System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
- System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

Skalowalność

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

Interoperacyjność

- System zarządzania tożsamością musi zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
- System zarządzania tożsamością musi zapewniać możliwość realizacji dwukierunkowej, uprawnionej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

Skalowalność funkcjonalna

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

Wymagania w zakresie cech i funkcjonalności rozwiązania

1. Agregacja i synchronizacja danych

a. System musi zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
b. System zarządzania tożsamością, w ramach początkowego wdrożenia musi zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
   - Pliki tekstowe CSV, AVP, LDIF
   - Bazy danych MS SQL 2000 - 2016, Oracle
   - Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.
c. System musi zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
d. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
e. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
f. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
h. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
i. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.

2. Repozytorium danych teleadresowych
   a. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
   b. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
   c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
   d. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.
3. Zarządzanie kartą elektroniczną
   a. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN'ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów),
   b. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników,
   c. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie)

d. System musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów dla jednego użytkownika)
e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp.,
f. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP,
g. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI,
h. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
i. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
j. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP,
k. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP,
l. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej),
m. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN'ami dostępowymi (zmiana PIN'u, odblokowanie karty),
n. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN'u inicjującego do karty elektronicznej następującymi drogami:
   - Użytkownik lub administrator wprowadza PIN inicjujący,
   - PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW,
   - System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku,
   - PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API),
o. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.
p. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego,
q. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN'u statycznego),
r. Na PIN'y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN'u, w szczególności:
   - nie mniej niż 6 znaków,
   - wymagane cyfry litery małe i duże,
   - PIN może się powtarzać przez N zmian,
s. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,
t. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego,
u. Workflow musi umożliwiać, implementacji następujących scenariuszy użycia:
   - w pełni automatyczne wystawianie certyfikatów dla użytkowników,
   - wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu,

- automatyczne odświeżanie wybranych certyfikatów,
- automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia,
- weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu,
- powiadamianie administratorów systemu o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej,

v. Wbudowane workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:
   - certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania,
   - certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW systemu,

Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych,

w. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN'ow, czy liczby odblokowanych kart,
x. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważnych,
y. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP" lub standard PKCS#11,
z. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania),

Podsystem zarządzania urządzeniami mobilnymi

1. Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
   a. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne
   b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
   c. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
   d. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:
      i. Nazwa urządzenia
      ii. Identyfikator urządzenia
      iii. Nazwa platformy systemu operacyjnego
      iv. Wersja oprogramowania układowego
      v. Typ procesora
      vi. Model urządzenia
      vii. Producent urządzenia
      viii. Architektura procesora
      ix. Język urządzenia
      x. Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
2. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).

3. Wymagania w zakresie dystrybucji oprogramowania:
   a. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
   b. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji
   c. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
   d. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:
      i. *. appx (Windows RT)
      ii. *.xap (Windows Phone 8)
      iii. *.ipa (iOS)
      iv. *.apk (Android)
   e. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:
      i. Windows Store
      ii. Windows Phone Store
      iii. Android Google Play Store
      iv. iOS App Store
4. W obszarze polityki haseł usługa zapewni:
      i. Zdefiniowanie wymuszenia hasła,
      ii. Określenie minimalnej długości hasła,
      iii. Określenie czasu wygasania hasła,
      iv. Określenie liczby pamiętanych haseł,
      v. Określenie liczby prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia,
      vi. Określenie czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła.
5. Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika:

Podsystem ochrony informacji

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

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
   a. Brak uprawnień dostępu do informacji,
   b. Informacja tylko do odczytu,
   c. Prawo do edycji informacji,
   d. Brak możliwości wykonania systemowego zrzutu ekranu,

   e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
   f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
   g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
6. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
7. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
8. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
9. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
10. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

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

2.1.2. Serwerowy system operacyjny z elementami zarządzania z prawem do aktualizacji typ I (licencja na 2 rdzenie procesora)

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.
1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. 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).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.
13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
18. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
22. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
23. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    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), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.

d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    i. Dystrybucję certyfikatów poprzez http
    ii. Konsolidację CA dla wielu lasów domeny,
    iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
j. Serwis udostępniania stron WWW.
k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
l. Wsparcie dla algorytmów Suite B (RFC 4869),
m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
q. Mechanizmy wirtualizacji mające wsparcie dla:
    i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    iii. Obsługi 4-KB sektorów dysków
    iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
    vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
25. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
26. Wsparcie dla rozwiązania Kubernetes.
27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
30. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
31. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

32. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
33. Mechanizm konfiguracji połączenia VPN do platformy Azure.
34. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
35. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
36. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Elementy zarządzania

Licencja musi uprawniać do zarządzania 2 (dwoma) środowiskami systemu operacyjnego na 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 wbudowane 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
2. 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.
3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.
    a. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika
    b. System powinien dawać możliwość integracji dostępnych zadań dystrybucji (pakietów instalacyjnych) z obsługą oprogramowania systemów Windows (dostępne do instalacji pakiety powinny się pojawiać w Panelu Sterowania w sekcji Dodaj/Usuń Programy, w części Dodaj Nowe Programy)

c. System powinien posiadać narzędzia pozwalające na przeskanowanie serwerów pod kątem zainstalowanych poprawek dla systemów operacyjnych Windows oraz dostarczać narzędzia dla innych producentów oprogramowania (ISVs) w celu przygotowania reguł skanujących i zestawów poprawek
d. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek
e. System powinien udostępniać informacje o aktualizacjach systemów operacyjnych Windows dostępnych na stronach producenta (Windows Update) oraz informacje o postępie instalacji tych aktualizacji na serwerach (również w postaci raportów)
System powinien również umożliwiać skanowanie i inwentaryzację poprawek, które były już instalowane wcześniej niezależnie od źródła dystrybucji
f. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil)
g. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie
h. System powinien zawierać wszystkie narzędzia do sporządzenia, modyfikacji i dystrybucji obrazów na dowolny komputer, również taki, na którym nie ma żadnego systemu operacyjnego (bare metal)
i. System powinien być zintegrowany z oprogramowaniem antywirusowym i być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.

4. 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 systemy komputerowego:
      - stan usługi (Windows Service)
      - obecność poprawek (Hotfix)
      - WMI
      - rejestr systemowy
      - system plików
      - Active Directory
      - SQL (query)
      - IIS Metabase
   c. Dla reguł sprawdzających system powinien dawać możliwość wprowadzenia wartości poprawnej, która byłaby wymuszana w przypadku odstępstwa lub wygenerowania alertu administracyjnego w sytuacji, kiedy naprawa nie jest możliwa.
5. 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 (inwentaryzacja)
      - Oprogramowanie (inwentaryzacja)
      - 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
   f. Konsola powinna zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:

- konfigurację granic systemu zarządzania
- konfigurację komponentów systemu zarządzania
- konfigurację metod wykrywania serwerów, użytkowników i grup
- konfigurację metod instalacji klienta
- konfiguracje komponentów klienta
- grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów)
- konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp…
- konfigurację reguł wykorzystania oprogramowania
- konfigurację zapytań (query) do bazy danych systemu
- konfiguracje raportów
- podgląd zdarzeń oraz zdrowia komponentów systemu.

6. 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. System zarządzania komponentami powinien składać się z:
        - Serwera Zarządzającego,
            - Serwer zarządzania jest punktem centralnym do zarządzanie grupą (pulą) serwerów i komunikowania się z bazą danych. Po otwarciu konsoli serwera możliwe jest podłączenie się do grupy zarządzającej, W zależności od wielkości środowiska komputerowego, grupa zarządzania może zawierać jeden lub wiele serwerów połączonych w pule zasobów.
        - Bazy Operacyjnej przechowującej informacje o zarządzanych elementach,
            - baza operacyjna jest relacyjną bazą danych, która zawiera wszystkie dane konfiguracyjne dla zarządzanej grupy serwerów i przechowuje wszystkie dane związane z monitorowaniem. Baza Operacyjna zachowuje dane krótkoterminowe, domyślnie 7 dni.
        - Baza Hurtowej przechowującej dane do analiz historycznych, definiuje granicę czasową do retencji danych historycznych.
    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.
    a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne 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 SP2
   - Windows 2008 Server SP2
   - Windows 2008 Server R2
   - Windows 2008 Server R2 SP1
   - Windows Server 2012
   - Windows Server 2012 R2
   - Windows Client OS:
     - Windows XP Pro x64 SP2
     - Windows XP Pro SP32
     - Windows Vista SP2
     - Windows XP Embedded Standard
     - Windows XP Embedded Enterprise
     - Windows XP Embedded POSReady
     - Windows 7 Professional for Embedded Systems
     - Windows 7 Ultimate for Embedded Systems
     - Windows 7

    - Windows 8
    - Windows 8.1
  - 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)
  - Information Worker (Office, IExplorer, Outlook, itp…)
  - IIS 6.0/7.0/7.5
  - Linux/Unix
    - HP-UX 11i V2 (PA-RISC and Itanium)
    - HP-UX 11i V3 (PA-RISC and Itanium)
    - Oracle Solaris 9 (SPARC)
    - Oracle Solaris 10 (SPARC and x86)
    - Oracle Solaris 11 (SPARC and x86)
    - Red Hat Enterprises Linux 4 (x86/x64)
    - Red Hat Enterprises Linux 5 (x86/x64)
    - Red Hat Enterprises Linux 6 (x86/x64)
    - SUSE Linux Enterprise Server 9 (x86)
    - SUSE Linux Enterprise Server 10 (x86/x64)
    - SUSE Linux Enterprise Server 11 (x86/x64)
    - IBM AIX 5.3 (POWER)
    - IBM AIX 6.1 (POWER)
    - IBM AIX 7.1 (POWER)
    - Cent OS 5 (x86/x64)
    - Cent OS 6 (x86/x64)
    - Debian 5 (x86/x64)
    - Debian 6 (x86/x64)
    - Ubuntu Server 10.04 (x86/x64)
    - Ubuntu Server 12.04 (x86/x64)
  - Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej np. Azure/AWS/Google

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 wykorzystanie 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 znajdą (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 dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).
7. Wymagania dodatkowe

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 utylizacji 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:
         i. profilu sprzętowego
         ii. profilu systemu operacyjnego,
         iii. 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 misi 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 automatyczne 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) musi spełniać następujące wymagania:

1. Architektura:
   a. System musi składać się z serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
   b. System musi posiadać agentów kopii zapasowych instalowanych na komputerach zdalnych
   c. System musi posiadać konsolę administracyjną instalowaną lokalnie na komputerach użytkowników zarządzających systemem
   d. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
2. Wykonywanie kopii zapasowych:
   a. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
   b. System kopii zapasowych musi posiadać możliwości zapisu danych na:
      i. na puli magazynowej złożonej z dysków twardych
      ii. na napędach I bibliotekach taśmowych
      iii. podłączonych zdalnie zasobach chmurowych

c. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych
d. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych
e. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
f. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
g. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.
h. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.
i. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony:
    i. Krótkoterminowe: Pule dyskowe – do 448 dni
    ii. Online: Zasoby chmurowe – do 3360 dni
    iii. Krótkoterminowe: Taśmy – do 12 tygodni
    iv. Długoterminowe: Taśmy – do 99 lat

3. Odzyskiwanie danych:
    a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje”
    b. System kopii zapasowych musi umożliwiać odtworzenie danych do:
        i. lokalizacji oryginalnej
        ii. lokalizacji alternatywnej
        iii. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych
4. Agent kopii zapasowej
    a. Agent powinien posiadać możliwość współpracy z komponentami VSC.
    b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych” oraz wykorzystywanego pasma w i poza godzinami „biznesowymi”
    c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:
        i. System operacyjny Windows (w tym pliki, system state i BMR)
        ii. Maszyny wirtualne na platformie Hyper-V
        iii. Bazy danych MS SQL
        iv. Sharepoint
        v. Exchange
5. Konsola administracyjna:
    a. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach
    b. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów
    c. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń

d. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych
e. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych
f. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać środowisko standaryzujące i automatyzujące zarządzanie procesami w systemach IT na bazie najlepszych praktyk.

1. Architektura:
   a. System musi posiadać graficzną konsolę dla administratorów (autorów) pozwalającą w łatwy sposób (bez znajomości języków programowania) tworzenie przebiegów procesów (runbooks) przy pomocy gotowych elementów aktywności.
   b. System musi posiadać tester przebiegów pozwalający na sprawdzenie poprawności wykonywania stworzonego przez administratora (autora) pokazując informacje o wykonaniu poszczególnych kroków, informacje wchodzące i wychodzące z poszczególnych kroków, możliwość ustawiania pułapek (breakpoints) oraz wykonywania krok po kroku.
   c. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.
   d. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).
   e. System powinien posiadać konsolę webową pozwalającą na podgląd zdefiniowanych przebiegów procesów, ich stanu, informacji historycznych o wykonanych przebiegach oraz pozwalająca na uruchamianie przebiegów procesów na żądanie.
   f. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).
2. Tworzenie przebiegów:
   a. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.
   b. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.
   c. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:
      i. System:
         1. Run Program
         2. Run .Net Script
         3. End Process
         4. Start/Stop Service
         5. Restart System
         6. Save Event Log
         7. Query WMI
         8. Run SSH Command
         9. Get SNMP Variable
         10. Monitor SNMP Trap
         11. Send SNMP Trap
         12. Set SNMP Variable
      ii. Planowanie:
         1. Monitor Date/Time
         2. Check Schedule
      iii. Monitorowanie:
         1. Monitor Event Log

2. Monitor Service
3. Get Service Status
4. Monitor Process
5. Get Process Status
6. Monitor Computer/IP Status
7. Monitor Disk Space
8. Get Disk Space Status
9. Monitor Internet Application
10. Get Internet Application Status
11. Monitor WMI

iv. Zarządzanie plikami:
1. Compress File
2. Copy File
3. Create Folder
4. Decompress File
5. Delete File
6. Delete Folder
7. Get File Status
8. Monitor File
9. Monitor Folder
10. Move File
11. Move Folder
12. PGP Decrypt File
13. PGP Encrypt File
14. Print File
15. Rename File

v. E-mail:
1. Send E-mail

vi. Powiadomienia:
1. Send Event Log Message
2. Send Syslog Message
3. Send Platform Event

vii. Narzędzia:
1. Apply XSLT
2. Query XML
3. Map Published Data
4. Compare Values
5. Write Web Page
6. Read Text Log
7. Write to Database
8. Query Database
9. Monitor Counter
10. Get Counter Value
11. Modify Counter
12. Invoke Web Services
13. Format Date/Time
14. Generate Random Text
15. Map Network Path
16. Disconnect Network Path
17. Get Dial-up Status
18. Connect/Disconnect Dial-up

viii. Zarządzanie plikami tekstowymi:

1. Append Line
2. Delete Line
3. Find Text
4. Get Lines
5. Insert Line
6. Read Line
7. Search and Replace Text

ix. Kontrola przepływów (runbooks):

1. Invoke Runbook
2. Initialize Data
3. Junction
4. Return Data

d. System powinien posiadać również inne zestawy aktywności, które mogą być zaimportowane na życzenie administratora (autora) w celu zarządzania procesami na innych systemach posiadanych przez zamawiającego, w tym:

x. Active Directory
xi. Exchange Admin
xii. Exchange Users
xiii. FTP Integration
xiv. HP iLO and OA
xv. HP Operations Manager
xvi. HP Service Manager
xvii. IBM Tivoli Netcool/OMNIbus
xviii. Representational State Transfer (REST)
xix. Sharepoint
xx. Microsoft Azure
xxi. VMware vSphere
xxii. System Center

3. Serwer zarządzający i baza danych:
   a. Serwer zarządzający powinien organizować jednoczesny dostęp konsoli graficznych administratorów i zapewniać funkcje Check-In/Check-Out dla poszczególnych przebiegów uniemożliwiając jednoczesne zmiany tego samego przebiegu przez dwóch użytkowników.
   b. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).
   c. Baza danych systemu powinna przechowywać:
      i. Definicje przebiegów procesów
      ii. Stan uruchomionych przebiegów
      iii. Informacje statusowe (logs)
      iv. Dane konfiguracyjne systemu

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi zapewniać zintegrowane środowisko pozwalające na uruchomienie usług wsparcia (service-desk) u zamawiającego.

1. Architektura:
   a. System musi posiadać serwer zarządzający odpowiedzialny za wykonywanie wszystkich zadań związanych z obsługą incydentów, problemów, zmian, zleceń, użytkowników, itp… zapewniając jednocześnie wymuszenie odpowiednich uprawnień.
   b. System musi posiadać zintegrowany komponent CMDB (Configuration Management Database)
   c. System musi posiadać zintegrowany moduł bazy wiedzy (Knowledge Management)
   d. System musi posiadać graficzną konsolę użytkownika instalowana lokalnie na komputerach pracowników wsparcia.

e. System musi posiadać komponent hurtowni danych, odpowiedzialny za agregację i przechowywanie danych historycznych i przygotowywanie raportów.
f. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
g. System musi posiadać konsolę webową umożliwiającą pracownikom zgłaszanie incydentów/problemów technicznych oraz zapotrzebowania na zasoby IT.

2. Procesy wsparcia:
   a. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy:
      i. Zarządzanie incydentami
      ii. Zarządzanie problemami
      iii. Zarządzanie zmianą
      iv. Zarządzanie
   b. W zakresie zarządzania incydentami i problemami system powinien posiadać:
      i. Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:
         - Narażony użytkownik,
         - Alternatywna metoda kontaktu,
         - Tytuł,
         - Opis,
         - Kategoria,
         - Pilność,
         - Wpływ,
         - Źródło,
         - Grupa pomocy technicznej,
         - Przypisany,
         - Podstawowy właściciel,
         - Uwzględnione usługi,
         - Narażone elementy,
         - Dziennik akcji (komentarz).

3. Komponent CMDB:
   a. Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym:
      i. Użytkownik:
         - Imię
         - Nazwisko
         - Inicjały
         - Tytuł,
         - Firma,
         - Dział,
         - Biuro,
         - Telefon służbowy,
         - Ulica i numer,
         - Miejscowość,
         - Województwo,
         - Kod pocztowy,
         - Kraj,
         - Strefa czasowa,
         - Ustawienia regionalne,
         - Komputery użytkownika
         - Urządzenia użytkownika
         - Elementy pokrewne (incydenty, problemy, zmiany, itp…)

ii. Komputer:

b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:
   i. Konektor do systemu zarządzania infrastrukturą i oprogramowaniem
   ii. Konektor do systemu zarządzania komponentami
   iii. Konektor do systemu zarządzania środowiskami wirtualnym
   iv. Konektor do systemu automatyzacji zarządzania środowisk IT
   v. Konektor do usługi katalogowej Active Directory

1. 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.
2. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
3. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
4. 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 exploity 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. 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.
7. 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.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. 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.).
10. 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.
11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

2.1.3. Serwerowy system operacyjny z elementami zarządzania z prawem do aktualizacji typ II (licencja na 2 rdzenie procesora)

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na wykorzystanie tej licencji w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. 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).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.

13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
18. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
22. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
23. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    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), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
j. Serwis udostępniania stron WWW.
k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
l. Wsparcie dla algorytmów Suite B (RFC 4869),
m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
q. Mechanizmy wirtualizacji mające wsparcie dla:
    i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    iii. Obsługi 4-KB sektorów dysków
    iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
    vii. Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

25. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
26. Wsparcie dla rozwiązania Kubernetes.
27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
30. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
31. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
32. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
33. Mechanizm konfiguracji połączenia VPN do platformy Azure.
34. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
35. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
36. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Elementy zarządzania

Licencja oprogramowania zarządzania środowiskami serwerowymi uprawniać do zarządzania nielimitowaną liczbą środowisk systemu operacyjnego na tym serwerze fizycznym.

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 wbudowane 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
2. 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.
3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.
    a. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika
    b. System powinien dawać możliwość integracji dostępnych zadań dystrybucji (pakietów instalacyjnych) z obsługą oprogramowania systemów Windows (dostępne do instalacji pakiety powinny się pojawiać w Panelu Sterowania w sekcji Dodaj/Usuń Programy, w części Dodaj Nowe Programy)
    c. System powinien posiadać narzędzia pozwalające na przeskanowanie serwerów pod kątem zainstalowanych poprawek dla systemów operacyjnych Windows oraz dostarczać narzędzia dla innych producentów oprogramowania (ISVs) w celu przygotowania reguł skanujących i zestawów poprawek
    d. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek
    e. System powinien udostępniać informacje o aktualizacjach systemów operacyjnych Windows dostępnych na stronach producenta (Windows Update) oraz informacje o postępie instalacji tych aktualizacji na serwerach (również w postaci raportów) System powinien również umożliwiać skanowanie i inwentaryzację poprawek, które były już instalowane wcześniej niezależnie od źródła dystrybucji
    f. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil)

g. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie
h. System powinien zawierać wszystkie narzędzia do sporządzenia, modyfikacji i dystrybucji obrazów na dowolny komputer, również taki, na którym nie ma żadnego systemu operacyjnego (bare metal)
i. System powinien być zintegrowany z oprogramowaniem antywirusowym i być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.

4. 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 systemy komputerowego:
      - stan usługi (Windows Service)
      - obecność poprawek (Hotfix)
      - WMI
      - rejestr systemowy
      - system plików
      - Active Directory
      - SQL (query)
      - IIS Metabase
   c. Dla reguł sprawdzających system powinien dawać możliwość wprowadzenia wartości poprawnej, która byłaby wymuszana w przypadku odstępstwa lub wygenerowania alertu administracyjnego w sytuacji, kiedy naprawa nie jest możliwa.
5. 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 (inwentaryzacja)
      - Oprogramowanie (inwentaryzacja)
      - 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
   f. Konsola powinna zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
      - konfigurację granic systemu zarządzania
      - konfigurację komponentów systemu zarządzania
      - konfigurację metod wykrywania serwerów, użytkowników i grup
      - konfigurację metod instalacji klienta
      - konfiguracje komponentów klienta
      - grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów)
      - konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp…
      - konfigurację reguł wykorzystania oprogramowania
      - konfigurację zapytań (query) do bazy danych systemu
      - konfiguracje raportów
      - podgląd zdarzeń oraz zdrowia komponentów systemu.
6. 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. System zarządzania komponentami powinien składać się z:
      - Serwera Zarządzającego,
        - Serwer zarządzania jest punktem centralnym do zarządzanie grupą (pulą) serwerów i komunikowania się z bazą danych. Po otwarciu konsoli serwera możliwe jest podłączenie się do grupy zarządzającej, W zależności od wielkości środowiska komputerowego, grupa zarządzania może zawierać jeden lub wiele serwerów połączonych w pule zasobów.
      - Bazy Operacyjnej przechowującej informacje o zarządzanych elementach,
        - baza operacyjna jest relacyjną bazą danych, która zawiera wszystkie dane konfiguracyjne dla zarządzanej grupy serwerów i przechowuje wszystkie dane związane z monitorowaniem. Baza Operacyjna zachowuje dane krótkoterminowe, domyślnie 7 dni.
      - Baza Hurtowej przechowującej dane do analiz historycznych, definiuje granicę czasową do retencji danych historycznych.
   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.
   j. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.
   k. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
   l. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
   m. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
   n. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
   o. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
   p. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
   q. Wsparcie dla protokołu IPv6.
   r. 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 SP2
   - Windows 2008 Server SP2
   - Windows 2008 Server R2
   - Windows 2008 Server R2 SP1
   - Windows Server 2012
   - Windows Server 2012 R2
   - Windows Client OS:
     - Windows XP Pro x64 SP2
     - Windows XP Pro SP32
     - Windows Vista SP2
     - Windows XP Embedded Standard
     - Windows XP Embedded Enterprise
     - Windows XP Embedded POSReady
     - Windows 7 Professional for Embedded Systems
     - Windows 7 Ultimate for Embedded Systems
     - Windows 7
     - Windows 8
     - Windows 8.1
   - 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)
   - Information Worker (Office, IExplorer, Outlook, itp…)
   - IIS 6.0/7.0/7.5
   - Linux/Unix
     - HP-UX 11i V2 (PA-RISC and Itanium)

- HP-UX 11i V3 (PA-RISC and Itanium)
- Oracle Solaris 9 (SPARC)
- Oracle Solaris 10 (SPARC and x86)
- Oracle Solaris 11 (SPARC and x86)
- Red Hat Enterprises Linux 4 (x86/x64)
- Red Hat Enterprises Linux 5 (x86/x64)
- Red Hat Enterprises Linux 6 (x86/x64)
- SUSE Linux Enterprise Server 9 (x86)
- SUSE Linux Enterprise Server 10 (x86/x64)
- SUSE Linux Enterprise Server 11 (x86/x64)
- IBM AIX 5.3 (POWER)
- IBM AIX 6.1 (POWER)
- IBM AIX 7.1 (POWER)
- Cent OS 5 (x86/x64)
- Cent OS 6 (x86/x64)
- Debian 5 (x86/x64)
- Debian 6 (x86/x64)
- Ubuntu Server 10.04 (x86/x64)
- Ubuntu Server 12.04 (x86/x64)

- Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej np. Azure/AWS/Google

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

a. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.
b. 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).
c. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.
d. 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 wykorzystanie 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 znajdą (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 dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).
7. Wymagania dodatkowe

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 utylizacji 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:
         i. profilu sprzętowego
         ii. profilu systemu operacyjnego,
         iii. 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 misi 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 automatyczne 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) musi spełniać następujące wymagania:

1. Architektura:
   a. System musi składać się z serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
   b. System musi posiadać agentów kopii zapasowych instalowanych na komputerach zdalnych
   c. System musi posiadać konsolę administracyjną instalowaną lokalnie na komputerach użytkowników zarządzających systemem
   d. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
2. Wykonywanie kopii zapasowych:
   a. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
   b. System kopii zapasowych musi posiadać możliwości zapisu danych na:
      i. na puli magazynowej złożonej z dysków twardych
      ii. na napędach I bibliotekach taśmowych
      iii. podłączonych zdalnie zasobach chmurowych
   c. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych
   d. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych
   e. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
   f. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych na

poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.

g. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.
h. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.
i. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony:
   i. Krótkoterminowe: Pule dyskowe – do 448 dni
   ii. Online: Zasoby chmurowe – do 3360 dni
   iii. Krótkoterminowe: Taśmy – do 12 tygodni
   iv. Długoterminowe: Taśmy – do 99 lat

3. Odzyskiwanie danych:
   a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje”
   b. System kopii zapasowych musi umożliwiać odtworzenie danych do:
      i. lokalizacji oryginalnej
      ii. lokalizacji alternatywnej
      iii. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych
4. Agent kopii zapasowej
   a. Agent powinien posiadać możliwość współpracy z komponentami VSC.
   b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych” oraz wykorzystywanego pasma w i poza godzinami „biznesowymi”
   c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:
      i. System operacyjny Windows (w tym pliki, system state i BMR)
      ii. Maszyny wirtualne na platformie Hyper-V
      iii. Bazy danych MS SQL
      iv. Sharepoint
      v. Exchange
5. Konsola administracyjna:
   a. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach
   b. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów
   c. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń
   d. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych
   e. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych
   f. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać środowisko standaryzujące i automatyzujące zarządzanie procesami w systemach IT na bazie najlepszych praktyk.

1. Architektura:

a. System musi posiadać graficzną konsolę dla administratorów (autorów) pozwalającą w łatwy sposób (bez znajomości języków programowania) tworzenie przebiegów procesów (runbooks) przy pomocy gotowych elementów aktywności.
b. System musi posiadać tester przebiegów pozwalający na sprawdzenie poprawności wykonywania stworzonego przez administratora (autora) pokazując informacje o wykonaniu poszczególnych kroków, informacje wchodzące i wychodzące z poszczególnych kroków, możliwość ustawiania pułapek (breakpoints) oraz wykonywania krok po kroku.
c. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.
d. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).
e. System powinien posiadać konsolę webową pozwalającą na podgląd zdefiniowanych przebiegów procesów, ich stanu, informacji historycznych o wykonanych przebiegach oraz pozwalająca na uruchamianie przebiegów procesów na żądanie.
f. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).

2. Tworzenie przebiegów:
    a. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.
    b. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.
    c. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:
        i. System:
            1. Run Program
            2. Run .Net Script
            3. End Process
            4. Start/Stop Service
            5. Restart System
            6. Save Event Log
            7. Query WMI
            8. Run SSH Command
            9. Get SNMP Variable
            10. Monitor SNMP Trap
            11. Send SNMP Trap
            12. Set SNMP Variable
        ii. Planowanie:
            1. Monitor Date/Time
            2. Check Schedule
        iii. Monitorowanie:
            1. Monitor Event Log
            2. Monitor Service
            3. Get Service Status
            4. Monitor Process
            5. Get Process Status
            6. Monitor Computer/IP Status
            7. Monitor Disk Space
            8. Get Disk Space Status
            9. Monitor Internet Application
            10. Get Internet Application Status
            11. Monitor WMI

iv. Zarządzanie plikami:
    1. Compress File
    2. Copy File
    3. Create Folder
    4. Decompress File
    5. Delete File
    6. Delete Folder
    7. Get File Status
    8. Monitor File
    9. Monitor Folder
    10. Move File
    11. Move Folder
    12. PGP Decrypt File
    13. PGP Encrypt File
    14. Print File
    15. Rename File
v. E-mail:
    1. Send E-mail
vi. Powiadomienia:
    1. Send Event Log Message
    2. Send Syslog Message
    3. Send Platform Event
vii. Narzędzia:
    1. Apply XSLT
    2. Query XML
    3. Map Published Data
    4. Compare Values
    5. Write Web Page
    6. Read Text Log
    7. Write to Database
    8. Query Database
    9. Monitor Counter
    10. Get Counter Value
    11. Modify Counter
    12. Invoke Web Services
    13. Format Date/Time
    14. Generate Random Text
    15. Map Network Path
    16. Disconnect Network Path
    17. Get Dial-up Status
    18. Connect/Disconnect Dial-up
viii. Zarządzanie plikami tekstowymi:
    1. Append Line
    2. Delete Line
    3. Find Text
    4. Get Lines
    5. Insert Line
    6. Read Line
    7. Search and Replace Text
ix. Kontrola przepływów (runbooks):
    1. Invoke Runbook
    2. Initialize Data

3. Junction
4. Return Data

d. System powinien posiadać również inne zestawy aktywności, które mogą być zaimportowane na życzenie administratora (autora) w celu zarządzania procesami na innych systemach posiadanych przez zamawiającego, w tym:
   x. Active Directory
   xi. Exchange Admin
   xii. Exchange Users
   xiii. FTP Integration
   xiv. HP iLO and OA
   xv. HP Operations Manager
   xvi. HP Service Manager
   xvii. IBM Tivoli Netcool/OMNIbus
   xviii. Representational State Transfer (REST)
   xix. Sharepoint
   xx. Microsoft Azure
   xxi. VMware vSphere
   xxii. System Center

3. Serwer zarządzający i baza danych:
   a. Serwer zarządzający powinien organizować jednoczesny dostęp konsoli graficznych administratorów i zapewniać funkcje Check-In/Check-Out dla poszczególnych przebiegów uniemożliwiając jednoczesne zmiany tego samego przebiegu przez dwóch użytkowników.
   b. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).
   c. Baza danych systemu powinna przechowywać:
      i. Definicje przebiegów procesów
      ii. Stan uruchomionych przebiegów
      iii. Informacje statusowe (logs)
      iv. Dane konfiguracyjne systemu

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi zapewniać zintegrowane środowisko pozwalające na uruchomienie usług wsparcia (service-desk) u zamawiającego.

1. Architektura:
   a. System musi posiadać serwer zarządzający odpowiedzialny za wykonywanie wszystkich zadań związanych z obsługą incydentów, problemów, zmian, zleceń, użytkowników, itp… zapewniając jednocześnie wymuszenie odpowiednich uprawnień.
   b. System musi posiadać zintegrowany komponent CMDB (Configuration Management Database)
   c. System musi posiadać zintegrowany moduł bazy wiedzy (Knowledge Management)
   d. System musi posiadać graficzną konsolę użytkownika instalowana lokalnie na komputerach pracowników wsparcia.
   e. System musi posiadać komponent hurtowni danych, odpowiedzialny za agregację i przechowywanie danych historycznych i przygotowywanie raportów.
   f. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
   g. System musi posiadać konsolę webową umożliwiającą pracownikom zgłaszanie incydentów/problemów technicznych oraz zapotrzebowania na zasoby IT.
2. Procesy wsparcia:
   a. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy:
      i. Zarządzanie incydentami
      ii. Zarządzanie problemami
      iii. Zarządzanie zmianą
      iv. Zarządzanie

b. W zakresie zarządzania incydentami i problemami system powinien posiadać:
   i. Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:
      - Narażony użytkownik,
      - Alternatywna metoda kontaktu,
      - Tytuł,
      - Opis,
      - Kategoria,
      - Pilność,
      - Wpływ,
      - Źródło,
      - Grupa pomocy technicznej,
      - Przypisany,
      - Podstawowy właściciel,
      - Uwzględnione usługi,
      - Narażone elementy,
      - Dziennik akcji (komentarz).

3. Komponent CMDB:
   a. Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym:
      i. Użytkownik:
         - Imię
         - Nazwisko
         - Inicjały
         - Tytuł,
         - Firma,
         - Dział,
         - Biuro,
         - Telefon służbowy,
         - Ulica i numer,
         - Miejscowość,
         - Województwo,
         - Kod pocztowy,
         - Kraj,
         - Strefa czasowa,
         - Ustawienia regionalne,
         - Komputery użytkownika
         - Urządzenia użytkownika
         - Elementy pokrewne (incydenty, problemy, zmiany, itp…)
      ii. Komputer:
   b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:
      i. Konektor do systemu zarządzania infrastrukturą i oprogramowaniem
      ii. Konektor do systemu zarządzania komponentami
      iii. Konektor do systemu zarządzania środowiskami wirtualnym
      iv. Konektor do systemu automatyzacji zarządzania środowisk IT
      v. Konektor do usługi katalogowej Active Directory

5. 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.

6. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
7. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
8. 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 exploity 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. 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.
7. 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.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. 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.).
10. 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.

11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

2.1.4. Serwer relacyjnej bazy danych z prawem do aktualizacji (licencja na 2 rdzenie procesora)

System bazodanowy (SBD) licencjonowany na rdzenie procesora musi spełniać poniższe wymagania poprzez wbudowane mechanizmy:

1. Możliwość wykorzystania SBD, jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Wykonywanie typowych zadań administracyjnych w trybie on-line - SBD musi umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy.
6. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
7. Skalowalność systemu - SBD powinien wspierać skalowanie w kontekście wielkości rozwiązania (powinien być dostępny zarówno na platformie wieloserwerowej, jak również średniej wielkości komputerów i urządzeń mobilnych).
8. Możliwość dodawania procesorów bez restartu systemu - SBD powinien umożliwiać dodanie procesora do systemu, bez konieczności restartu silnika bazy danych.
9. Kopie bazy tylko do odczytu - SBD powinien umożliwiać tworzenie w dowolnym momencie kopii bazy danych tylko do odczytu zawierającej stan bazy z bieżącego momentu czasu. Wiele takich kopii może być równolegle użytkowanych w celu wykonywania z nich zapytań.
10. Możliwość dodawania pamięci bez restartu systemu - SBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych.
11. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych.
12. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między wieloma lokalizacjami (podstawowa i zapasowe) przy zachowaniu następujących cech:
    - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
    - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
    - duplikacja danych w trybie synchronicznym lub asynchronicznym,
    - SBD musi umożliwiać duplikację danych z ośrodka podstawowego, do co najmniej 8 lokalizacji zapasowych,

- w celu zwiększenia skalowalności i wydajności systemu SBD musi umożliwiać korzystanie z kopii baz w lokalizacjach zapasowych w trybie tylko do odczytu (raportowanie, tworzenie backupów itp.) bez przerywania działania mechanizmu duplikacji danych z ośrodka podstawowego,
- klienci bazy danych mogą być automatycznie przełączeni do bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
- brak limitu odległości między systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza oraz limity wynikające z opóźnień na łączu),
- kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenie 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).

13. Replikacja danych i modyfikacja w wielu punktach - SBD 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 SBD powinien umożliwiać kompresję przesyłanych danych między serwerami uczestniczącymi w replikacji, aby minimalizować obciążenie łączy sieciowych.
14. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
15. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania powinien wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
16. Możliwość szyfrowania przechowywanych danych - SBD musi pozwalać na szyfrowanie przechowywanych danych. Szyfrowanie musi być cechą SBD i nie może wymagać jakichkolwiek zmian w aplikacjach korzystających z danych. Zaszyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zaszyfrowana.
17. Korzystanie z zewnętrznych urządzeń do przechowywania kluczy szyfrujących - SBD powinien posiadać mechanizm pozwalający na 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 SBD.
18. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.
19. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
20. Ograniczenie użycia zasobów – SBD powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, % wykorzystania pamięci, liczba operacji wejścia/wyjścia podsystemu dyskowego). Reguły definiujące ograniczenia dla użytkowników lub grup użytkowników dotyczące wykorzystania zasobów powinny mieć możliwość

użycia w nich logiki zaimplementowanej za pomocą języka programowania (np. używanego w danym SBD języka SQL).

21. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
22. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
23. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych powinien udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).
24. System SDB musi łączyć w sobie cechy bazy przechowywanej w pamięci RAM (IMDB) oraz tradycyjnej bazy danych (RDBMS) przechowywanej na dyskach.
25. System SDB musi zapewniać w ramach tej samej bazy danych możliwość umieszczenia wybranych tabel w pamięci RAM serwera, a pozostałych tabel w tradycyjnej postaci (na dysku).
26. SBD musi posiadać możliwość korzystania w procedurach jednocześnie z tabel przechowywanych w pamięci RAM oraz tabel przechowywanych na dyskach.
27. System SDB musi zapewniać wersjonowanie wierszy w tabelach przechowywanych w pamięci RAM.
28. W celu zwiększenia wydajności SBD musi posiadać możliwość tworzenia procedur składowanych w kodzie natywnym, to znaczy takich procedur, które są automatycznie kompilowane do kodu natywnego podczas ich tworzenia oraz składają się z instrukcji procesora, które nie wymagają dalszych kompilacji lub interpretacji.
29. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu). Wymagana jest rejestracja zdarzeń:
    - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (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 (w celu wychwytywania długotrwałych blokad obiektów bazy).
30. Możliwość rejestrowania bardzo dużej liczby zdarzeń i analizowania ich z minimalnym opóźnieniem – SBD powinien dostarczać wbudowaną platformę do tworzenia aplikacji typu CEP (Complex Event Processing). Aplikacje takie umożliwiają rejestrowanie bardzo dużej liczby zdarzeń (np. odczytów liczników lub z innych urządzeń pomiarowych, dowolnych zdarzeń występujących z dużą częstotliwością) i reagowanie na nie z minimalnym opóźnieniem. System powinien również udostępniać mechanizmy wysokiej dostępności dla tej usługi.
31. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
32. Definiowanie nowych typów danych - SBD musi 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 okrojenia typów wbudowanych lub ich kombinacji.
33. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:

- 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.

34. Wsparcie dla danych przestrzennych - SBD musi 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,
    - 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 SBD,
    - 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.).
35. Możliwość efektywnego przechowywania dużych obiektów binarnych - SBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty, itp.). Obiekty te nie powinny być przechowywane w plikach bazy danych, ale w systemie plików. Jednocześnie pliki te powinny być zarządzane przez SBD (kontrola dostępu na podstawie uprawnień nadanych w SBD). Dodatkowo dane binarne powinny być dostępne dla użytkowników bazy danych jako standardowa kolumna tabeli (dostęp z poziomu zapytań języka SQL obsługiwanego przez SBD).
36. Możliwość kompresji przechowywanych danych - SBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych w celu osiągnięcia lepszej wydajności przy niezmienionej konfiguracji sprzętowej. System kompresji powinien umożliwiać również kompresję UNICODE systemem UCS-2.
37. Możliwość rejestracji zmiany w rekordzie danych – SBD 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.
38. Audyt dostępu do danych - SBD 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 SBD.
39. Partycjonowanie danych - SBD powinien pozwalać na podział danych w jednej tabeli między różne fizyczne pamięci masowe zgodnie ze zdefiniowanymi warunkami podziału. 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).

40. Wsparcie dla Indeksów kolumnowych - SBD powinien umożliwiać tworzenie indeksów przechowujących dane osobno dla każdej z kolumn tabeli łącząc je następnie w całość. Indeks powinien również wykorzystywać mechanizm kompresji oraz pozwalać na modyfikowanie danych w tabeli, dla której taki indeks utworzono.
41. Indeksowanie podzbioru danych w tabeli - SBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.
42. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.
43. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
44. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
45. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
46. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.
47. System transformacji danych - SBD musi 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 przerwano 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 podmiany źródła danych,
- możliwość integracji z transakcjami bazy danych SBD, także rozproszonymi bez potrzeby pisania kodu.

48. Wbudowany system analityczny - SBD musi 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.
49. Wbudowany system analityczny musi 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 rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. System powinien pozwalać na integrację z relacyjną bazą danych –wymagana jest możliwość uruchomienia procesu wyliczenia agregacji zainicjowana poprzez dodanie rekordu do tabeli w relacyjnej bazy danych. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
50. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
51. Narzędzia do zarządzania jakością danych - SBD powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:
    - udostępniać funkcje do profilowania danych (analiza i raporty dotyczące jakości danych),
    - udostępniać funkcje do deduplikacji danych,
    - określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną do akceptacji przez użytkownika,
    - 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 oraz ewentualnie te przed korektą,
    - 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).

52. Możliwość zarządzania centralnymi słownikami danych - SBD 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,
    - umożliwiać wersjonowanie danych (śledzenie 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.
53. Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
54. Wbudowany system analityczny musi 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).
55. Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
56. Wbudowany system analityczny powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.
57. Wbudowany system analityczny powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.
58. Wbudowany system analityczny 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.
59. Wbudowany system analityczny 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.
60. Wbudowany system analityczny powinien dostarczać kreatory modelowania złożonych procesów biznesowych, pozwalających w prosty sposób niezaawansowanym użytkownikom implementować złożone problemy analizy biznesowej w modelu analitycznym, czyniąc programowanie projektów BI przystępnym dla większej liczby osób i organizacji.
61. Wsparcie dla optymalizacji zapytań z modelu gwiazdy (fakty-wymiary) - SBD 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).
62. Wsparcie dla zapytań aktualizujących tabele faktów w modelach wielowymiarowych - SBD 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.

63. Aktywne buforowanie danych Proactive caching - SBD powinien udostępniać mechanizm odświeżania danych w strukturach wielowymiarowych, który wykrywa zmiany w systemach źródłowych i na bieżąco aktualizuje bazę wielowymiarową.
64. Wbudowany system analityczny powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane).
65. Wbudowany system analityczny 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.
66. Wbudowany system analityczny 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.
67. Wbudowany system analityczny 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).
68. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
69. System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining.
70. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators) - SBD musi 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.
71. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie 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) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
    - możliwość wizualizacji wskaźników KPI,
    - możliwość wizualizacji danych w postaci obiektów sparkline.
72. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
73. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.

74. SBD musi 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.
75. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).
76. Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
77. Narzędzia do tworzenia raportów ad-hoc - SBD 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.

2.1.5. Subskrypcja pakietu zarządzania projektami - subskrypcja na użytkownika

Subskrypcja usługi zarządzania projektami pozwalająca na:

1. Możliwość wyboru języka interfejsu użytkownika, w tym języka polskiego i angielskiego.
2. Dostępność usługi na poziomie 99,9%.
3. Obecność tzw. klauzul umownych Unii Europejskiej (EU Model Clauses) w umowie na wykorzystanie usługi.
4. Zagwarantowane w usłudze mechanizmy składowania danych (backup) i ich odtwarzania.
5. Zarządzanie zadaniami projektowymi,
6. Współdzielenie dokumentów projektowych,
7. Synchronizację zadań projektowych z portalem wielofunkcyjnym,
8. Dystrybucję kart czasu pracy.
9. Zarządzania projektami.
10. Wykorzystanie środowiska portalu wielofunkcyjnego jako interfejsu użytkownika.
11. Współdziałanie z kalendarzami systemu Exchange w zakresie przepływu informacji o zadaniach i ich aktualizacji, z wyłączeniem informacji typu out-of-office (poza biurem).
12. Wykorzystanie otwartego standardu OData do wyszukiwania danych i ich analizy.
13. Dane dotyczące realizowanych projektów i dokumentacja projektowa muszą być przechowywane w sposób bezpieczny z ochroną dostępu dla uprawnionych osób. System ma umożliwić dostęp do aktualnego statusu prowadzonych projektów.
14. Możliwość wykorzystania profili użytkowników lub ich grup z usługi katalogowej przy udzielaniu uprawnień dostępu.
15. Kontrola, rozpatrywanie i zatwierdzanie dokumentów za pomocą definiowalnego przepływu pracy (workflow),
16. Możliwość definiowania przepływu pracy przy pomocy oprogramowania Visio.
17. 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 odpowiedzialności za realizację poszczególnych zadań i projektów,
18. Dostęp do funkcji systemu poprzez przeglądarkę Internet Explorer (wersja 8 lub wyższa), Firefox, Safari i Chrome.
19. Możliwość definiowania projektów za pomocą pakietu zarządzania projektami (niezależnego narzędzia instalowanego na stacjach klienckich).

Usługa 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 opóźnienia zadania względem planu bazowego
    - Informacja czy jest plan bazowy,
    - Informacja o odchyleniu względem czasu,
    - Informacja o odchylenia 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

Usługa musi zapewniać dostępność instalacji pakietu zarządzania projektami, zapewniającego 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. 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 spływającymi 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 opóźnienia zadania względem planu bazowego
    a. Informacja czy jest plan bazowy,
    b. Informacja o odchyleniu względem czasu,
    c. Informacja o odchylenia 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 serwera zarządzania projektami – pełna, dwukierunkowa synchronizacja danych.
24. Możliwość przypisywania zasobów z Active Directory.

2.1.6. Subskrypcja pakietu modelowania graficznego - subskrypcja na użytkownika

Pakiet usług do graficznego modelowania w postaci wektorowej: procesów biznesowych, procesów obiegu informacji, schematów organizacyjnych, diagramów sieciowych, harmonogramów wraz możliwością instalacji pakietu na komputerze klasy PC. Pakiet musi zapewniać:

1. Możliwość otwierania i przeglądania rysunków przy użyciu bezpłatnie dostępnego narzędzia.
2. Zgodność z interfejsem dotykowym Windows.
3. Możliwość pracy kilku osób na jednym diagramie w tym samym czasie.
4. Zapis danych w postaci plików XML.
5. Zgodność ze standardami:
    a. Unified Modeling Language (UML) 2.4,
    b. Business Process Model and Notation (BPMN) 2.0.
6. Publikacja przepływów pracy dla SharePoint.
7. Możliwość importu i eksportu do formatu plików zgodnych z AutoCad.
8. Możliwość graficznego obrazowania i analizowania danych pobieranych z plików xls i xlsx, baz danych dostępnych przez ODBC na diagramach.
9. Udostępnianie kreatorów budowy diagramów.
10. Udostępnianie gotowych kształtów (shape) opisanych metadanymi i możliwość kreowania i edycji kształtów.
11. Możliwość zmiany kształtu przy zachowaniu jego metadanych oraz całości diagramu.
12. Możliwość budowy diagramów przestawnych, które są kolekcją kształtów uporządkowanych w strukturę drzewa, która pomaga analizować dane i podsumowywać je w zrozumiałym formacie wizualnym. Taki diagram zaczyna się od kształtu nazywanego węzłem najwyższego poziomu, który zawiera informacje zaimportowane z arkusza, tabeli, widoku lub modułu. Węzeł najwyższego poziomu można podzielić na poziom węzłów podrzędnych, aby dane można było wyświetlać w różny sposób.
13. Udostępnianie gotowych szablonów służących do wizualizowania i usprawniania procesów biznesowych, śledzenia projektów i zasobów, układania schematów organizacji, mapowania sieci, tworzenia diagramów obszarów budowy i optymalizacji systemów. Wymagane są szablony graficznego modelowania w postaci wektorowej:
    a. procesów biznesowych,
    b. procesów obiegu informacji,
    c. schematów organizacyjnych,
    d. diagramów sieciowych,
    e. harmonogramów.
14. Funkcja autołączenia, która automatycznie łączy kształty, równomiernie je rozmieszcza i wyrównuje do założonej siatki. Przenoszenie połączonych kształtów nie rozłącza ich, tylko powoduje automatyczne wytyczenie nowej trasy łącznika między nimi.
15. Połączenie diagramów z danymi umożliwiające uzyskanie obrazu procesu, projektu lub systemu pozwalające na identyfikowanie kluczowych trendów, problemów i wyjątków, a następnie określanie właściwego sposobu postępowania.
16. Graficzne raporty z informacjami o projektach do wizualizacji kompleksowych informacji o projektach. Umożliwienie generowania raportów, które pozwalają śledzić informacje o zadaniach, właścicielach, rolach i obowiązkach dotyczących projektów, a także przedstawiają złożone struktury własności w projekcie.

17. Możliwość automatycznego modyfikowania raportów w miarę zmian informacji o projektach.

2.1.7. Pakiet usług wsparcia technicznego

Pakiet wsparcia technicznego musi obejmować swoim zakresem świadczenie opieki serwisowej oprogramowania i usług producenta oferowanych produktów w okresie trwania subskrypcji.
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 poszukiwania 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.

1. Wymagana jest dostawa subskrypcji pakietu wsparcia technicznego, który zapewni:
   a. Świadczenie usługi w zakresie organizacji i koordynacji usług w zakresie wsparcia technicznego oferowanego oprogramowania.
   b. Usługi w zakresie wsparcia technicznego świadczone przez okres 36 miesięcy od dnia podpisania umowy.
   c. Zapewni możliwość bezpośredniego zgłaszania problemów technicznych do producenta oprogramowania lub spółki zależnej producenta (Producenta) drogą elektroniczną poprzez dedykowaną stronę Producenta i telefonicznie.
   d. Zagwarantuje możliwość wykonywania poprawek do oprogramowania (HotFix) przez Producenta.
2. Warunki świadczenia usług w zakresie wsparcia technicznego Produktów:
   a. Usługi w zakresie wsparcia technicznego (Produktów) mają obejmować 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).

b. Wymagane jest świadczenie usług mających 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.
c. 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.
d. W ramach usług wsparcia technicznego Zamawiający wymaga przedstawienia oferty na standardowe pakiety wsparcia technicznego zawierające 600 godzin roboczych (do 200 godzin rocznie) możliwych do wykorzystania w okresie trwania umowy.
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 w Polsce (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. „d." powyżej.
h. Pakiet usług 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 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, przeglądanym i uaktualnianym 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.

Wymagany sposób realizacji usług w przypadku wystąpienia problemu:

Waga Problemu	Sytuacja	Oczekiwana Reakcja	Oczekiwana Reakcja Klienta
1 wyłącznie zgłoszenie telefoniczne	• Katastrofalny wpływ na działalność: • Podstawowe procesy biznesowe (mission critical) przestały funkcjonować i nie można w rozsądny sposób kontynuować pracy • Konieczna natychmiastowa pomoc	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 1 godzina • Pracownicy Producenta wysłani do lokalizacji Klienta tak szybko, jak to będzie możliwe • Praca w systemie 24 godziny przez 7 dni w tygodniu • Błyskawiczna eskalacja do zespołów Produktowych Producenta • Powiadomienie kierownictwa wyższego szczebla Producenta	• Powiadomienie kierownictwa wyższego szczebla Klienta • Przydzielenie odpowiednich zasobów w celu umożliwienia prowadzenia prac w systemie 24 godziny przez 7 dni w tygodniu • Szybki dostęp i czas reakcji władz kontrolujących zmiany
A Wyłącznie zgłoszenie telefoniczne	• Krytyczny wpływ na działalność: • Znacząca utrata lub obniżenie jakości usług • Wymaga pomocy w ciągu 1 godziny	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 1 godzina • Pracownicy Producenta wysłani do lokalizacji Klienta tak szybko, jak to będzie możliwe • Prace w systemie 24 godziny przez 7 dni w tygodniu • Powiadomienie kierownictwa Producenta wyższego szczebla	• Przydzielenie odpowiednich zasobów w celu umożliwienia prowadzenia prac w systemie 24 godziny przez 7 dni w tygodniu • Szybki dostęp i czas reakcji władz kontrolujących zmiany • Powiadomienie kierownictwa
B Zgłoszenie telefonicznie lub za pośrednictwem Internetu	• Umiarkowany wpływ na działalność: • Umiarkowana utrata lub obniżenie jakości usług, jednakże praca może być kontynuowana bez zakłóceń • Wymaga pomocy w ciągu 2 Godzin Roboczych	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 2 godziny • Prace realizowane wyłącznie w Godzinach Roboczych	• Przydzielenie odpowiednich zasobów w celu umożliwienia prowadzenia ciągłych prac w Godzinach Roboczych[1] • Dostęp i reakcja władz kontrolujących zmiany w ciągu 4 Godzin Roboczych
C Zgłoszenie telefonicznie lub za pośrednictwem Internetu	• Minimalny wpływ na działalność: • Działalność prowadzona praktycznie z niewielkimi zakłóceniami lub bez zakłóceń • Wymaga pomocy w ciągu 4 Godzin Roboczych	• Odpowiedź na pierwszy telefon w czasie nie dłuższym niż 4 godziny • Prace realizowane wyłącznie w Godzinach Roboczych	• Podanie dokładnych informacji kontaktowych • Reakcja w ciągu 24 godzin.

3. Porady Techniczne:
   Porady Techniczne muszą obejmować krótkoterminowe udzielanie porad i wskazówek w związku z problemami nieobjętymi Usługami Wsparcia Technicznego. Do Porad Technicznych zalicza się również krótkoterminowe usługi konsultacyjne dotyczące kwestii związanych z projektowaniem, rozwojem i wdrożeniami. Pracownik Producenta podejmie współpracę z Zamawiającym w celu określenia indywidualnych potrzeb Klienta w zakresie Porad Technicznych.

Następujące Porady Techniczne mogą być wykorzystane na podstawie niniejszego Opisu Usług:

a. Porady dotyczące Infrastruktury. Porady dotyczące Infrastruktury obejmują udzielanie porad, wskazówek i przekazywanie wiedzy w celu umożliwienia Zamawiającemu wdrożenia technologii Producenta w sposób pozwalający uniknąć powszechnych trudności technicznych i zmniejszyć ryzyko wystąpienia nieprzewidzianych awarii i przestojów w pracy systemów.

Usługi te pomagają Zamawiającemu także w rozwiązywaniu problemów niezwiązanych z Produktami, w tym:

- Błędów spowodowanych przez infrastrukturę sieciową Zamawiającego, sprzęt, oprogramowanie innych dostawców, procedury operacyjne, architekturę, procesy zarządzania usługami IT, konfigurację systemu lub błędy ludzkie.
- Problemów związanych ze zgodnością i koordynacją produktów wielu dostawców. Na żądanie Zamawiającego Wykonawca nawiąże współpracę z dostawcami oprogramowania będącymi osobami trzecimi w celu rozwiązania złożonych problemów związanych z brakiem zgodności produktów różnych dostawców.

b. Analizy. Analiza ma być oceną określonego systemu, aplikacji lub architektury mającą na celu ustalenie kwestii związanych z projektowaniem, rozwojem, wdrożeniem oraz możliwością wsparcia technicznego w odniesieniu do dotychczasowych lub planowanych wdrożeń technologii Producenta. Zakres każdej analizy będzie ustalany indywidualnie oraz oszacowany przed przydzieleniem zasobów. Efektem analizy ma być sporządzenie pisemnego raportu celem udokumentowania ustaleń i zaleceń.

c. Wsparcie dla Programistów. Wsparcie dla Programistów ma zapewnić Zamawiającemu opracowywanie i rozwijanie wewnętrznych aplikacji na platformach Producenta. Wsparcie dla Programistów obejmuje przede wszystkim narzędzia programistyczne i technologie Producenta.

d. Dostęp do Laboratorium. Zamawiający wymaga możliwości zapewnienia dostępu do laboratorium w ramach pomocy dotyczącej opracowywania produktu, testowania, przygotowywania wersji wstępnych oraz działań migracyjnych Produktów.

4. Usługi Informacyjne.

W ramach Usług Informacyjnych Zamawiający wymaga dostępu do informacji technicznych na temat Produktów oraz narzędzi wsparcia, które mają za zadanie pomóc w efektywnym i skutecznym wdrożeniu oraz używaniu Produktów. Usługi Informacyjne mają obejmować dowolne połączenie poniższych usług:

a. Witryna sieciowa zapewniająca bezpłatny dostęp do następujących zasobów informacyjnych:
   - Regularnie aktualizowane informacje o produktach zawierające kluczowe informacje na temat wsparcia i obsługi Produktów.
   - Ostrzeżenia informujące Zamawiającego o potencjalnie poważnych problemach.

b. Aplikacja internetowa umożliwiająca zgłaszanie i sprawdzanie statusu zgłoszonych Incydentów.
   - Baza wiedzy Producenta zawierająca artykuły techniczne i narzędzia oraz wskazówki dotyczące rozwiązywania problemów.

c. Transmisje dot. Wsparcia. Transmisje dot. wsparcia mają zapewnić regularnie odbywające się dyskusje „na żywo” za pośrednictwem Internetu, prowadzone przez kierowników programowych Producenta, programistów i ekspertów głównie na tematy związane z technologiami Producenta.

Część „B”

1. Wymagania w zakresie dostaw

Przedmiotem zamówienia jest subskrypcja pakietu platformy usług hostowanych (dalej łącznie nazywanych Produktem)w ramach 36-cio miesięcznej umowy.

Oferowany Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).

Zamawiający wymaga dostawy Produktu na warunkach przewidzianych przez producenta Produktów (Producenta) dla jednostek Skarbu Państwa.

W związku z faktem, iż Zamawiający przewiduje prawo opcji w niniejszym zamówieniu, Zamawiający gwarantuje dokonanie zakupu w ramach zamówienia podstawowego Produktu w liczbie określonej w kolumnie „Liczba Produktu gwarantowana” i przewiduje, w ramach prawa opcji, możliwość zakupu łącznie Produktu wymienionych w kolumnach „Liczba Produktu opcjonalnego” w pierwszym, drugim lub trzecim roku trwania umowy.

Specyfikacja ilościowa przedmiotu zamówienia:

Lp.	**Typ oprogramowania**	Liczba produktów gwarantowanych	Liczba produktów opcjonalnych
1.	Subskrypcja pakietu platformy usług hostowanych (jednostek/36 miesięcy)	720	720

Tabela 1 – specyfikacja ilościowa zamawianego produktu.

1.1. Wymagania ogólne

1. Zamawiający wymaga zagwarantowania niezmienności cen Producenta na Produkt w całym okresie trwania umowy, z wyłączeniem zmian kursowych EUR/PLN.
2. Zamawiający wymaga od Wykonawcy dedykowania do obsługi umowy co najmniej 2 osób, posiadających wiedzę, z zakresu pól eksploatacji Produktu.
3. Oferowane subskrypcje usług hostowanych muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i normatywów potwierdzonych aktualnymi wynikami niezależnych audytów, w szczególności:
    a) ISO 27001, ISO 27002, ISO 27017, ISO 27018
    b) UK G-Cloud
    c) SOC 1, SOC 2
    d) Open Authentication Standard – OAuth
4. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:
    a. Zarządzanie tymi usługami/Produktami,
    b. Monitorowanie stanu utylizacji i kosztów Produktów,
5. Zamawiający wymaga udzielenia uprawnień na stronie Producenta w terminie do 10 dni roboczych od podpisania umowy.
6. Po dziewięćdziesięciu (90) dniach od zakończenia okresu trwania umowy Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Producenta i usunięcie jego danych.

7. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
8. Jeżeli nowa wersja Produktu zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego Produktu przez Zamawiającego.

2. Specyfikacja techniczno – eksploatacyjna

Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenie pełnej zgodności oferowanych produktów z wymogami specyfikacji. Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy.

2.1. Subskrypcja pakietu platformy usług hostowanych

Subskrypcja standardowej, powszechnie dostępnej przez Internet platformowej usługi hostowanej typu COTS (Commercial Of-The-Shelf) polegająca na udostępnieniu skalowalnej platformy pozwalającej wykorzystać w formie usługi serwerowe systemy operacyjne, silniki baz danych oraz inne aplikacje w środowiskach zwirtualizowanych.

1. Usługa ta ma posiadać następujące parametry:
    - 1.1. Udostępnienie skalowalnej platformy pozwalającej wykorzystać w formie usługi serwerowe systemy operacyjne, silniki baz danych oraz inne aplikacje w środowiskach zwirtualizowanych.
    - 1.2. Dostępność usługi w okresie trwania umowy:
        - 1.2.1. Minimum 1 jednostka obliczeniowa o parametrach 1 rdzeń procesora, 1,7GB RAM, pod kontrolą systemu operacyjnego Windows Server lub Linux (wybrane dystrybucje), w okresie dostępności usługi.
        - 1.2.2. Minimum 70 GB dostępnej lokalnie redundantnej przestrzeni dyskowej.
        - 1.2.3. Minimum 100 GB transferu danych do i z platformy usługi hostowanej.
    - 1.3. Gwarantowana dostępność usług platformy na poziomie 99,9%.
    - 1.4. Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług platformy.
    - 1.5. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
    - 1.6. Możliwość wyboru różnych rodzajów dysków i ich pojemności.
    - 1.7. Możliwość uruchomienia aplikacji internetowych wykorzystujących technologię ASP.NET, PHP, Java, Python z automatyczną dystrybucją ruchu sieciowego HTTP pomiędzy kilka pracujących serwerów.
    - 1.8. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów z możliwością zdalnego dostępu.
    - 1.9. Możliwość analizy danych gromadzonych w czasie rzeczywistym i danych historycznych.
    - 1.10. Komunikacja z usługą poprzez REST API.
    - 1.11. Zbieranie danych operacyjnych z wykorzystaniem dedykowanego oprogramowania – agenta,
    - 1.12. Kompatybilność w zakresie monitorowania i zarządzania z Microsoft System Center Operations Manager.
    - 1.13. Narzędzia tworzenia aplikacji mobilnych spełniające następujące wymagania (opcjonalnie dostępnych w ramach usługi):
        - 1.13.1. Wsparcie dla urządzeń z systemem klienckim Windows, Windows Phone, iOS, Android oraz HTML5.
        - 1.13.2. Wsparcie po stronie platformy dla JavaScript i .Net.

1.13.3. Integracja z serwisami notyfikacji i uwierzytelniania.
1.13.4. Obsługa wysyłania poczty elektronicznej email.
1.13.5. Obsługa skryptów i zadań wg harmonogramu.
1.13.6. Możliwość gromadzenia logów i monitorowania usługi.

1.14. Możliwość przechowywania danych spełniająca następujące wymagania w ramach usługi:
1.14.1. Wysoka skalowalność, auto-partycjonowanie, load-balancing.
1.14.2. Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka.
1.14.3. Wsparcie dla systemów klienckich Windows i Linux.
1.14.4. Skalowalność pojedynczego zasobu pamięci 500TB.
1.14.5. Replikacja danych - min. 3 kopie w ramach pojedynczej lokalizacji.
1.14.6. Replikacja z lokalizacji podstawowe do innej lokalizacji znajdującej się również na terenie Europejskiego Obszaru Gospodarczego.
1.14.7. Udostępnienie zasobów pamięci poprzez REST API.
1.14.8. Gotowe biblioteki programistyczne środowisk programowania: .NET, Java/Android, Node.js, PHP, Ruby, Python, PowerShell.

1.15. Dostępność usług umożliwiających uruchamianie aplikacji WWW w modelu gotowej do wykorzystania usługi, z utrzymywanymi przez dostawcę usług komponentami infrastruktury i możliwości w pełni automatycznego skalowania. Usługi te powinny zapewniać możliwość uruchamiania aplikacji działających w minimum następujących technologiach: ASP .NET, PHP, Python, Java.

1.16. Dostępność relacyjnej i nierelacyjnej bazy danych, w tym oparte o technologię Hadoop, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.

1.17. Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a dostawcą Platformy w technologii MPLS.

1.18. Możliwość dostarczenia dedykowanego urządzenia stanowiącego lokalny magazyn przechowywania danych, podłączony do chmury z funkcją deduplikacji, szyfrowania i hierarchizacji pamięci, objętego wsparciem dostawcy Platformy.

1.19. Możliwość serializacji do określonego formatu tekstowego (np. opartego o XML lub JSON) rozwiązań opartych o maszyny wirtualne, wraz z ich konfiguracją, w sposób umożliwiający ich automatyczną deserializację i utworzenie na tej podstawie gotowego do pracy środowiska.

A. Dostępność funkcjonalności umożliwiającej oszacowanie kosztów usług hostowych

1. Oparcie się o usługi typu subskrypcji standardowej, powszechnie dostępnej przez Internet platformowej usługi hostowanej typu COTS (Commercial Of-The-Shelf) o przewidywalnym koszcie określonym jasnymi zasadami wyceny.
2. Dostępność funkcjonalności pozwalającej na oszacowanie kosztów wykorzystania usługi platformy.
3. Możliwość zmiany wymaganych parametrów usługi i jej skalowania zgodnie z potrzebami.
4. Możliwość automatycznego skalowania mocy obliczeniowej platformy.
5. Zużycie jednostek usług hostowanych za faktyczne wykorzystanie usług platformy z możliwością ich okresowego wyłączania.
6. Dostępność funkcjonalności pozwalającej na bieżące monitorowanie wykorzystania usług Platformy.

B. Zgodność ze standardami

1. Dostępność narzędzi wspomagających migrację aplikacji i danych zarówno ze środowisk własnych do Platformy, jak i z Platformy na dowolną inną platformę opartą o standard serwerów X64, a więc pozwalających na przeniesienie usług w przypadku podjęcia takiej decyzji.
2. Zastosowanie w Platformie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, w szczególności:

- ISO 27001, ISO 27002, ISO 27017, ISO 27018.
- UK G-Cloud.
- SOC 1, SOC 2.
- TDS (tabular data stream).
- Open Authentication Standard – OAuth. - OData.

W zakresie interoperacyjności
- HTTP(S) – TLS.
- Docker.
- REST API.

W zakresie programowania:
- Java.
- .NET.
- PHP.
- Python.
- Node.js.
- Wsparcie narzędziowe w Visual Studio i Eclipse.

3. Wsparcie Platformy dla standardowych rozwiązań OpenSource takich jak WordPress, Joomla, Drupal, OrchardCMS, MediaWiki, phpBB czy Mojo. Dostępność w ramach platformy predefiniowanych obrazów z tym oprogramowaniem.

C. Dostępność systemów i ich bezpieczeństwo
1. Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym).
2. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy.
3. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
4. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi.
5. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego.
6. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
7. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single signon) na bazie własnej usługi katalogowej Active Directory.
8. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
9. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
10. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych.
11. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN).
12. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS.
13. Przynajmniej dwa równorzędne ośrodki przetwarzania danych na terytorium krajów Europejskiego Obszaru Gospodarczego oddalone od siebie o co najmniej 100 km.

D. Zgodność z obowiązującym prawem Polskim i Unijnym
1. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego.
2. Zgodność usługi z rozp. RODO i potwierdzenie roli operatora usługi jako współprzetwarzającego dane.

3. Zapisy umowne zawierające tzw. Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych,
4. Wszelkie dane przetwarzane/składowane przez Zamawiającego w usłudze danych pozostają wyłączną własnością Zamawiającego.
5. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
6. Gwarancja usunięcia danych Zamawiającego z Platformy po zakończeniu Umowy.
7. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.
8. Gwarancja usunięcia danych w terminie 180 dni od wygaśnięcia subskrypcji i zakończenia umowy

Prawo opcji

1. Zamawiający na podstawie art. 34 ust. 5 Ustawy Pzp przewiduje zastosowanie prawa opcji.
2. Realizacja prawa opcji polegać będzie na:
   2.1. Zwiększeniu ilości subskrypcji usług komunikacyjnych, bezpieczeństwa i oprogramowania klasy desktop (subskrypcja na użytkownika) do 1.500 sztuk,
   2.2. Zwiększeniu ilości serwerowych systemów operacyjnych z elementami zarządzania z prawem do aktualizacji typ I (licencja na 2 rdzenie procesora) do 64 sztuk,
   2.3. Zwiększeniu ilości serwerowych systemów operacyjny z elementami zarządzania z prawem do aktualizacji typ II (licencja na 2 rdzenie procesora) do 32 sztuk,
   2.4. Zwiększeniu ilości serwerów relacyjnej bazy danych z prawem do aktualizacji (licencja na 2 rdzenie procesora) do 32 sztuk,
   2.5. Zwiększeniu ilości subskrypcji pakietu zarządzania projektami do 5 sztuk,
   2.6. Zwiększeniu ilości subskrypcji pakietu modelowania graficznego do 5 sztuk,
   2.7. Zwiększeniu ilości subskrypcji pakietu platformy usług hostowanych (jednostek/36 miesięcy) do 720 sztuk.

   w stosunku do ilości zamówienia podstawowego, również w sytuacji wyczerpania kwoty maksymalnej umowy, przeznaczonej na zrealizowanie zamówienia podstawowego.
3. Prawo opcji realizowane będzie na takich samych warunkach jak zamówienie podstawowe.
4. Ceny jednostkowe produktów wymienionych w pkt 2.1 – 2.7, zamawianych w ramach prawa opcji, będą identyczne jak zamówienia podstawowego, określone w Formularzu oferty złożonym przez Wykonawcę (załącznik nr 2 do SIWZ).
5. Zamawiający będzie mógł skorzystać z prawa opcji w sytuacji, gdy wykorzystane zostaną ilości pierwotne, wskazane w opisie przedmiotu zamówienia.
6. Jeśli w danej pozycji przedmiotu zamówienia wykorzystana zostanie ilość przewidziana w zamówieniu podstawowym, zamawiający będzie mógł zamawiać dalej, aż do wykorzystania ilości przewidzianych jako opcja.
7. Zamawiający skorzysta z prawa opcji do upływu terminu obowiązywania umowy na realizację przedmiotu zamówienia.
8. O zamiarze skorzystania z prawa opcji Zamawiający poinformuje Wykonawcę odrębnym pismem/oświadczeniem z określeniem zakresu, w jakim Zamawiający będzie z prawa opcji korzystał.
9. Produkty zamawiane w ramach prawa opcji muszą spełniać wymagania techniczne opisane w Załączniku Nr 1 do SIWZ „Opisie przedmiotu zamówienia”. Do dostawy produktów w ramach prawa opcji

zastosowanie mają postanowienia określające warunki i sposób zapłaty wynagrodzenia, warunki dostarczenia i odbioru, gwarancji oraz kar umownych.

10. Zamawiający nie ma obowiązku korzystać z prawa opcji. Wykonawcy nie przysługuje prawo roszczeń z tytułu niewykorzystania prawa opcji lub jego pełnej wartości.