Warunki równoważności dotyczące znaków towarowych.

Spis treści

1. SharePoint

System równoważny do Sharepoint musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

1. Publikacji dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych dostępnych przez przeglądarkę internetową;
2. Tworzenia witryn www;
3. Tworzenia repozytoriów – bibliotek przechowywania treści i plików;
4. Publikowania forów dyskusyjnych z oceną treści i publikacją własnych treści;
5. Publikowania ankiet;
6. Udostępniania formularzy elektronicznych;
7. Tworzenia repozytoriów wzorów dokumentów;
8. Tworzenia repozytoriów dokumentów;
9. Zarządzania strukturą portalu, witrynami, treściami www, repozytoriami plików i uprawnieniami użytkowników;
10. Zakładania przez użytkowników własnych struktur – witryn, repozytoriów;
11. Tworzenia spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról i grup ról użytkowników wraz z określaniem praw dostępu na bazie usługi katalogowej;
12. Wspólnej, bazującej na niezaprzeczalnych uprawnieniach pracy nad dokumentami;
13. Wersjonowania dokumentów;
14. Zarządzania mechanizmami ewidencjonowania i wyewidencjonowania dokumentów (blokowania dokumentu do wyłącznych praw edycji lub odblokowywania wyłącznych praw edycji);
15. Możliwość pracy z dokumentami w formacie XML w oparciu schematy XML przechowywane w repozytoriach portalu;
16. Organizacji pracy grupowej, poprzez udostępnianie użytkownikom wymienionych mechanizmów funkcjonalnych do których dana grupa ma uprawnienia;
17. Wyszukiwania treści zarówno poprzez wyszukiwanie fraz jak i metadanych dokumentów z możliwością ich filtrowania;
18. Dostępu do danych w relacyjnych bazach danych z zachowaniem uprawnień użytkownika do konkretnego zakresu danych;
19. Możliwości analizy danych wraz z graficzną prezentacją danych;
20. Możliwości wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning);
21. Budowy struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali (podportali), które w zależności od nadanych uprawnień mogą być zarządzane niezależnie i prezentować wspólne lub różne treści;
22. Nadawania uprawnień użytkownikom lub ich grupom wspólnie dla całej struktury portalu (z prawami dziedziczenia w strukturze), lub też niezależnie dla każdego podportalu, witryny czy repozytorium w zakresie zarządzania strukturą i treściami i nadawania dalszych uprawnień;
23. Nadawania gotowych typów uprawnień (administrator, zapisywanie i odczyt, tylko odczyt) i definiowanie własnych zakresów uprawnień dla użytkowników lub grup użytkowników;
24. Wsparcia pracy zespołowej poprzez definiowalne mechanizmy przepływów pracy (workflow) pozwalających na tworzenie obiegów dokumentów i spraw wraz z funkcjonalnością integracji przepływów z web-services, wywoływania web-services z poziomu workflow;
25. Mechanizmy wspierające przepływy pracy (workflow) bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu;
26. Możliwość instalacji serwera na maszynach fizycznych i maszynach wirtualnych w środowiskach własnych i hostowanych;

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

1. Interfejs użytkownika:
   a. Dostęp za pomocą standardowej przeglądarki internetowej (Microsoft Explorer, Microsoft Edge, Opera, Safari);
   b. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu repozytoria dokumentów, kalendarze oraz bazy kontaktów;

c. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego, np. edytora tekstu;
d. Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu, poprzez mechanizmy replikacji aktualnego stanu repozytorium i dokumentów na zasób lokalny przy każdym uzyskaniu połączenia z portalem;
e. Wbudowane zasady pozwalające na konfigurację zgodną z WCAG 2.0;
f. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy);

2. Bezpieczeństwo:
   a. Szyfrowanie połączeń TLS 1.1 i 1.2;
   b. Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP;
   c. Uwierzytelnianie użytkowników na bazie oświadczeń (claim-based authentication) z wykorzystaniem:
      i. SAML (Security Assertion Markup Language);
      ii. Windows claims;
      iii. Na bazie formularzy – Forms based claims;
   d. Uwierzytelniania aplikacji i stowarzyszonego użytkownika na bazie tokenów;
   e. Uwierzytelniania z poziomu serwera na bazie Open Authorization 2.0;
   f. Uwierzytelnianie za pomocą pojedynczego logowania domenowego użytkowników zdefiniowanych w zaimplementowanej usłudze katalogowej (single-sign on);
   g. Możliwość uruchomienia mechanizmu wyszukiwania danych wrażliwych w zasobach portalu (takich jak numery kart kredytowych, PESEL, numery dowodów osobistych czy paszportów) z powiadamianiem właścicieli zasobów lub/i administratorów portalu;
   h. Narzędzia zabezpieczania i monitorowania udostępnionych innym użytkownikom zasobów:
      i. Monitorowanie udostępnionych folderów i plików;
      ii. Definicja przypomnień przy zapomnieniu hasła;
      iii. Wskazanie użytkownika udostępniającego folder;
      iv. Wysyłanie wiadomości pocztą elektroniczną do użytkowników zapraszanych do korzystania z folderu;
      v. Mechanizm wnioskowania o dostęp do udziału i mechanizm akceptacji/odrzucenia wniosku dla administrującego zasobem;
      vi. Możliwość wykorzystania różnych portów SMTP poza standardowym 25;

3. 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;
   e. Mechanizm „przypinania” przez użytkownika odwiedzanych stron portalu do zestawu stron za którym podąża;

4. Integracja z innymi aplikacjami producenta portalu 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 systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili;
   d. Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony);
   e. Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego;
   f. Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services;

g. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym opartym o zewnętrzną (niewbudowaną) relacyjną bazę danych;

5. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:
   a. Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania;
   b. Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML);
   c. Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego;
   d. Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów;
   e. Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte;
   f. Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana;
   g. Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny);
   h. Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo;
6. Organizacja i publikacja treści:
   a. Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści;
   b. Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla odbiorców. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed udostępnieniem jej wszystkim odbiorcom;
   c. Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji;
   d. Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące hierarchię struktury.
   e. Automatyczne generowanie mapy stron portalu;
   f. Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi;
   g. Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu;
   h. Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT;
   i. Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji;
   j. Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji;
   k. Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu;

7. Repozytoria dokumentów:
   a. Możliwość publikacji dokumentów w intranecie przez edytorów portalu poprzez ich tworzenie, kopiowanie lub zapis z pakietu biurowego;
   b. Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa;
   c. Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu;
   d. Możliwość publikacji plików w strukturze katalogów;
   e. Możliwość publikacji materiałów wideo oraz audio;
   f. Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku;
   g. Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów;
   h. Elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania;
   i. Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), wraz z automatyczną kontrola wersji przy publikacji dokumentów;
   j. Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów wraz informacją dla użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i mechanizmem pozwalającym podjąć decyzję o ich publikacji lub odrzuceniu;
   k. Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.
   l. Wbudowany dwupoziomowy kosz na usuwane dokumenty;
   m. Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów z wbudowanymi politykami zabezpieczającymi przed natychmiastowym usunięciem dokumentu z kosza;
   n. Możliwość automatyzacji usuwania duplikatów dokumentów;
8. Wyszukiwanie treści:
   a. Pełnotekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice;
   b. Centralny mechanizm wyszukiwania treści dostępny dla uprawnionych użytkowników;
   c. Wyświetlanie w wynikach wyszukiwania jedynie tych zasobów, do których użytkownik ma uprawnienia;
   d. Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji;
   e. Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów;
   f. Możliwość definiowania słownika słów wykluczonych (często używanych);
   g. Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu;
   h. Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu,
      i. Podgląd zawartości plików graficznych, video, dokumentów pakietu biurowego i wyglądu stron;
         w wynikach wyszukiwania;
      j. Przedstawianie w wynikach duplikatów plików;
      k. Statystyki wyszukiwanych fraz;
9. Administracja intranetem i inne funkcje:
   a. Narzędzia wsparcia instalacji w postaci farmy portali z wydzielonymi ich rolami – przynajmniej 3 role: Serwer aplikacji, Serwer Cache, Front-end serwer;
   b. Narzędzia wsparcia instalacji dla modelu hybrydowego – własnej instalacji farmy portalu uzupełnionej funkcjami portalu z chmury producenta portalu;
   c. Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla

administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych;
d. Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu;
e. Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści;
f. Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i usługi webservice oraz wykorzystywania ich do opisywania dokumentów;
g. Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu;
h. Dostępność statystyk odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie – dostępność zaawansowanych statystyk i analiz odwiedzin;

2. System Center

System równoważny do System Center musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

A. System zarządzania infrastrukturą i oprogramowaniem;
B. System zarządzania komponentami;
C. System zarządzania środowiskami wirtualnym;
D. System tworzenia kopii zapasowych;
E. System automatyzacji zarządzania środowisk IT;
F. System zarządzania incydentami i problemami;
G. Ochrona antymalware;

A. 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 dystrybucję 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:
      1) stan usługi (Windows Service);
      2) obecność poprawek (Hotfix);
      3) WMI;
      4) rejestr systemowy;
      5) system plików;
      6) Active Directory;
      7) SQL (query);
      8) 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:
      1) Sprzęt (inwentaryzacja);
      2) Oprogramowanie (inwentaryzacja);
      3) Oprogramowanie (wykorzystanie);
      4) 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:
      1) konfigurację granic systemu zarządzania;
      2) konfigurację komponentów systemu zarządzania;
      3) konfigurację metod wykrywania serwerów, użytkowników i grup;
      4) konfigurację metod instalacji klienta;

5) konfiguracje komponentów klienta;
6) grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów);
7) konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp.;
8) konfigurację reguł wykorzystania oprogramowania;
9) konfigurację zapytań (query) do bazy danych systemu;
10) konfiguracje raportów;
11) 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;

B. 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:
      1) 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;
      2) 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;
      3) Bazy 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;
   d. 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;
   e. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług;
   f. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych;
   g. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny;
   h. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych;
   i. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany;
   j. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN);
   k. Wsparcie dla protokołu IPv6;
   l. 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:
      1) Rejestru;
      2) WMI;
      3) OLEDB;
      4) LDAP;
      5) 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:
      1) Windows Server 2003 SP2;
      2) Windows 2008 Server SP2;
      3) Windows 2008 Server R2;
      4) Windows 2008 Server R2 SP1;
      5) Windows Server 2012;
      6) Windows Server 2012 R2;
      7) Windows Client OS:
         a. Windows XP Pro x64 SP2;
         b. Windows XP Pro SP32;
         c. Windows Vista SP2;
         d. Windows XP Embedded Standard;
         e. Windows XP Embedded Enterprise;
         f. Windows XP Embedded POSReady;
         g. Windows 7 Professional for Embedded Systems;
         h. Windows 7 Ultimate for Embedded Systems;
         i. Windows 7;
         j. Windows 8;
         k. Windows 8.1;
      8) Active Directory 2003/2008;
      9) Exchange 2003/2007/2010;
      10) Microsoft SharePoint 2003/2007/2010;
      11) Microsoft SharePoint Services 3.0;
      12) Microsoft SharePoint Foundation 2010;
      13) SQL 2005/2008/2008R2 (x86/x64/ia64);
      14) Information Worker (Office, IExplorer, Outlook, itp.);
      15) IIS 6.0/7.0/7.5;
      16) Linux/Unix:
         a. HP-UX 11i V2 (PA-RISC and Itanium);
         b. HP-UX 11i V3 (PA-RISC and Itanium);
         c. Oracle Solaris 9 (SPARC);
         d. Oracle Solaris 10 (SPARC and x86);
         e. Oracle Solaris 11 (SPARC and x86);
         f. Red Hat Enterprises Linux 4 (x86/x64);
         g. Red Hat Enterprises Linux 5 (x86/x64);
         h. Red Hat Enterprises Linux 6 (x86/x64);
         i. SUSE Linux Enterprise Server 9 (x86);
         j. SUSE Linux Enterprise Server 10 (x86/x64);
         k. SUSE Linux Enterprise Server 11 (x86/x64);

l. IBM AIX 5.3 (POWER);
m. IBM AIX 6.1 (POWER);
n. IBM AIX 7.1 (POWER);
o. Cent OS 5 (x86/x64);
p. Cent OS 6 (x86/x64);
q. Debian 5 (x86/x64);
r. Debian 6 (x86/x64);
s. Ubuntu Server 10.04 (x86/x64);
t. Ubuntu Server 12.04 (x86/x64);

17) 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:
   1) interfejsy sieciowe;
   2) porty;
   3) sieci wirtualne (VLAN);
   4) grupy Hot Standby Router Protocol (HSRP);
f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
   1) SNMP (trap, probe);
   2) WMI Performance Counters;
   3) Log Files (text, text CSV);
   4) Windows Events (logi systemowe);
   5) Windows Services;
   6) Windows Performance Counters (perflib);
   7) WMI Events;
   8) Scripts (wyniki skryptów, np.: WSH, JSH);
   9) Unix/Linux Service;
   10) 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:
      1) Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event);
      2) Performance based (SNMP performance, WMI performance, Windows performance);
      3) 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:
      1) na ilość takich samych próbek o takiej samej wartości;
      2) 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:
      1) ASP .Net Application;
      2) ASP .Net Web Service;
      3) OLE DB;
      4) TCP Port;
      5) Web Application;
      6) Windows Service;
      7) Unix/Linux Service;
      8) 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:
      1) XML;
      2) CSV;
      3) TIFF;
      4) PDF;
      5) XLS;
      6) 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:
      1) w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna);
      2) 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:
      1) Alerts;
      2) Events;
      3) State;
      4) Performance;
      5) Diagram;
      6) Task Status;
      7) 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:
1) opcji definiowania ról użytkowników;
2) opcji definiowania widoków;
3) opcji definiowania i generowania raportów;
4) opcji definiowania powiadomień;
5) opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących;
6) 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:
a. Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo);
b. Wykonywanie operacji w systemie z poziomu linii poleceń;
c. Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania;
d. Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio)
z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie;

C. System zarządzania środowiskami wirtualnym:

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura:
a. System zarządzania środowiskiem wirtualnym powinien składać się z:
1) serwera zarządzającego;
2) relacyjnej bazy danych przechowującej informacje o zarządzanych elementach;
3) konsoli, instalowanej na komputerach operatorów;
4) portalu self-service (konsoli webowej) dla operatorów „departamentowych”;
5) biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych;
6) agenta instalowanego na zarządzanych hostach wirtualizacyjnych;
7) „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:
a) profilu sprzętowego;
b) profilu systemu operacyjnego;

c) przygotowanych dysków twardych;
b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania;
c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:
1) w trybie migracji „on-line" – bez przerywania pracy;
2) 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;

2) 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:
1) utylizacja poszczególnych hostów;
2) trend w utylizacji hostów;
3) alokacja zasobów na centra kosztów;
4) utylizacja poszczególnych maszyn wirtualnych;
5) komputery-kandydaci do wirtualizacji;
d. System musi umożliwiać skorzystanie z szablonów:
1) wirtualnych maszyn;
2) usług;
oraz profili dla:
1) aplikacji;
2) serwera SQL;
3) hosta;
4) sprzętu;
5) 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);

D. 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:
1) na puli magazynowej złożonej z dysków twardych;
2) na napędach I bibliotekach taśmowych;
3) 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:
   1) Krótkoterminowe: Pule dyskowe – do 448 dni;
   2) Online: Zasoby chmurowe – do 3360 dni;
   3) Krótkoterminowe: Taśmy – do 12 tygodni;
   4) 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:
      1) lokalizacji oryginalnej;
      2) lokalizacji alternatywnej;
      3) 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:
      1) System operacyjny Windows (w tym pliki, system state i BMR);
      2) Maszyny wirtualne na platformie Hyper-V;
      3) Bazy danych MS SQL;
      4) Sharepoint;
      5) 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.);

E. 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:
      1) System:
         a) Run Program;
         b) Run .Net Script;
         c) End Process;
         d) Start/Stop Service;
         e) Restart System;
         f) Save Event Log
         g) Query WMI;
         h) Run SSH Command;
         i) Get SNMP Variable;
         j) Monitor SNMP Trap;
         k) Send SNMP Trap;
         l) Set SNMP Variable;
      2) Planowanie
         a) Monitor Date/Time
         b) Check Schedule
      3) Monitorowanie:
         a) Monitor Event Log
         b) Monitor Service
         c) Get Service Status
         d) Monitor Process
         e) Get Process Status
         f) Monitor Computer/IP Status
         g) Monitor Disk Space
         h) Get Disk Space Status
         i) Monitor Internet Application
         j) Get Internet Application Status
         k) Monitor WMI
      4) Zarządzanie plikami:
         a) Compress File
         b) Copy File
         c) Create Folder
         d) Decompress File
         e) Delete File
         f) Delete Folder

g) Get File Status
h) Monitor File
i) Monitor Folder
j) Move File
k) Move Folder
l) PGP Decrypt File
m) PGP Encrypt File
n) Print File
o) Rename File

5) E-mail:
   a) Send E-mail
6) Powiadomienia:
   a) Send Event Log Message
   b) Send Syslog Message
   c) Send Platform Event
7) Narzędzia:
   a) Apply XSLT
   b) Query XML
   c) Map Published Data
   d) Compare Values
   e) Write Web Page
   f) Read Text Log
   g) Write to Database
   h) Query Database
   i) Monitor Counter
   j) Get Counter Value
   k) Modify Counter
   l) Invoke Web Services
   m) Format Date/Time
   n) Generate Random Text
   o) Map Network Path
   p) Disconnect Network Path
   q) Get Dial-up Status
   r) Connect/Disconnect Dial-up
8) Zarządzanie plikami tekstowymi:
   a) Append Line
   b) Delete Line
   c) Find Text
   d) Get Lines
   e) Insert Line
   f) Read Line
   g) Search and Replace Text
9) Kontrola przepływów (runbooks):
   a) Invoke Runbook
   b) Initialize Data
   c) Junction
   d) 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:
   1) Active Directory;
   2) Exchange Admin;
   3) Exchange Users;
   4) FTP Integration;
   5) HP iLO and OA;
   6) HP Operations Manager;
   7) HP Service Manager;
   8) IBM Tivoli Netcool/OMNIbus;

9) Representational State Transfer (REST);
10) Sharepoint;
11) Microsoft Azure;
12) VMware vSphere;
13) 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:
      1) Definicje przebiegów procesów;
      2) Stan uruchomionych przebiegów;
      3) Informacje statusowe (logs);
      4) Dane konfiguracyjne systemu;

F. 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:
      1) Zarządzanie incydentami;
      2) Zarządzanie problemami;
      3) Zarządzanie zmianą;
      4) Zarządzanie;
   b. W zakresie zarządzania incydentami i problemami system powinien posiadać:
      1) Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:
         a) Narażony użytkownik;
         b) Alternatywna metoda kontaktu;
         c) Tytuł;
         d) Opis;
         e) Kategoria;
         f) Pilność;
         g) Wpływ;
         h) Źródło;
         i) Grupa pomocy technicznej;
         j) Przypisany;
         k) Podstawowy właściciel;
         l) Uwzględnione usługi;
         m) Narażone elementy;
         n) 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:
   1) Użytkownik:
      a) Imię;
      b) Nazwisko;
      c) Inicjały;
      d) Tytuł;
      e) Firma;
      f) Dział;
      g) Biuro;
      h) Telefon służbowy;
      i) Ulica i numer;
      j) Miejscowość;
      k) Województwo;
      l) Kod pocztowy;
      m) Kraj;
      n) Strefa czasowa;
      o) Ustawienia regionalne;
      p) Komputery użytkownika;
      q) Urządzenia użytkownika;
      r) Elementy pokrewne (incydenty, problemy, zmiany, itp.);
   2) Komputer:
b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną
   i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:
   1) Konektor do systemu zarządzania infrastrukturą i oprogramowaniem;
   2) Konektor do systemu zarządzania komponentami;
   3) Konektor do systemu zarządzania środowiskami wirtualnym;
   4) Konektor do systemu automatyzacji zarządzania środowisk IT;
   5) Konektor do usługi katalogowej Active Directory;

4. 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;
5. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami;
6. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie;
7. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
   a. Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką;
   b. Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia;
   c. Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu;
   d. Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
   e. Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniu systemu w przypadku incydentów;
   f. Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej;
   g. Tworzenie baz wiedzy na temat rozwiązywania problemów;
   h. Automatyzację działań w przypadku znanych i opisanych problemów;
   i. Wykrywanie odchyleń od założonych standardów ustalonych dla systemu;

G. 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;

3. Active Directory:

1. System równoważny do Active Directory musi spełniać następujące wymagania:
   a) umożliwia scentralizowane zarządzanie obiektami AD (serwery, drukarki czy udostępnione pliki), a także przypisywanie uprawnień do tychże zasobów;
   b) umożliwiająca uwierzytelnienie obiektów (np. użytkowników, komputerów) i autoryzacja (lub jej odmowa) dostępu do innych obiektów Active Directory (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji;
   c) umożliwia konfigurację obiektów AD;
   d) możliwość działania w rozproszonych sieciach;
   e) możliwość działania w środowisku Microsoft Windows Server;
   f) możliwość konfiguracji za pomocą narzędzi graficznych i z linii komend;
   g) możliwość tworzenia skryptów;
   h) wykorzystuje LDAP (Lightweight Directory Access Protocol);
2. Obiekty AD:
   a) Konto użytkownika – obiekt zawierający informacje o użytkowniku;
   b) Kontakt – obiekt zawierający informacje kontaktowe użytkowników;
   c) Komputer – obiekt zawierający informacje o komputerze;
   d) Drukarka – obiekt zawierający odniesienie (wskaźnik) do drukarek sieciowych;
   e) Udział sieciowy – obiekt zawierający odniesienie do udostępnionych folderów w sieci;
   f) Grupa – obiekt zawierający kolekcję innych obiektów AD, stosowany do zarządzania uprawnieniami
   g) Jednostka organizacyjna – obiekt administracyjny obejmujący inne obiekty AD, stasowany do zarządzania konfiguracją;
   h) Domena AD – podstawowa struktura Active Directory, w ramach której zdefiniowane są pozostałe obiekty;

i) Kontroler Domeny – obiekt zawierający informację o serwerze pełniącym funkcję kontrolera AD;
j) Lokalizacja (Site) – obiekt zawierający informację o podsieciach w danej lokalizacji;
k) Builtin – grupy o predefiniowanych uprawnieniach do wykonywania czynności administracyjnych;
l) Relacja zaufania – obiekt zawierający informację o relacjach zaufania pomiędzy domenami AD;

4. Hyper-V

System równoważny do Hyper-V musi spełniać następujące wymagania:

1. możliwość uruchomienia w systemach Windows 8, 10 i Windows Server 2012 i 2016;
2. możliwość uruchamiania maszyn wirtualnych 32-bitowych i 64-bitowych;
3. możliwość konfiguracja klastra wysokiej dostępności;
4. możliwość przenoszenia maszyn wirtualnych bez przerw w działaniu;
5. możliwość obsługi do 1TB RAM na hoście;
6. możliwość realizacji zadań w interfejsie graficznym i z linii komend;
7. możliwość obsługi pamięci dynamicznej;
8. możliwość importu i eksportu maszyn wirtualnych;
9. możliwość śledzenia i gromadzenia dane dotyczące użycia zasobów fizycznych — procesora, pamięci, magazynu i sieci — przez określone maszyny wirtualne;
10. możliwość replikowania maszyn wirtualnych między systemami magazynowania, klastrami i centrami danych znajdującymi się w dwóch lokacjach, zapewniając ciągłość działalności biznesowej i funkcje odzyskiwania danych po awarii;
11. możliwość przypisania karty sieciowej, która obsługuje wirtualizację we/wy z jednym elementem głównym bezpośrednio do maszyny wirtualnej;
12. możliwość przenoszenia wirtualnych dysków twardych używanych przez maszynę wirtualną do innego magazynu fizycznego, gdy maszyna wirtualna jest uruchomiona;
13. możliwość magazynowania maszyn wirtualnych przy użyciu udziałów plików SmB 3.0;
14. możliwość bezpośredniego łączenia się z magazynem Fibre Channel z systemu operacyjnego gościa uruchomionego na maszynie wirtualnej;
15. po usunięciu migawki maszyny wirtualnej miejsce zajmowane przez nią w magazynie jest udostępniane w czasie działania maszyny wirtualnej.

5. Windows Server

System równoważny do Windows Serwer musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym;
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny;
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych;
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci;
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy;
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy;
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego;
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
9. 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);

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość;
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji;
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET;
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów;
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych;
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy;
    b. dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych;
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji;
18. 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);
19. 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;
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu;
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa;
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management);
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
25. 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:
        1) podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną;
        2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania;
        3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza;
        4) 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;
    e. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        1) dystrybucję certyfikatów poprzez http;
        2) konsolidację CA dla wielu lasów domeny;
        3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen;
        4) 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. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów;
i. serwis udostępniania stron WWW;
j. wsparcie dla protokołu IP w wersji 6 (IPv6);
k. wsparcie dla algorytmów Suite B (RFC 4869);
l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows;
m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
    1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych;
    2) obsługi ramek typu jumbo frames dla maszyn wirtualnych;
    3) obsługi 4-KB sektorów dysków;
    4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra;
    5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API;
    6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode);

26. 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;
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath);
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego;
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF;
31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim;

6. Technologia .NET

Technologia równoważna do Technologii .NET musi spełniać następujące wymagania:

1) może być hostowana przez niezarządzane składniki, które ładują środowisko uruchomieniowe języka wspólnego do swoich procesów i inicjują wykonywanie kodu zarządzanego, tworząc w ten sposób środowisko oprogramowania korzystające z funkcji zarządzanych i niezarządzanych;
2) hostuje środowisko uruchomieniowe w celu zapewnienia skalowalnego środowiska po stronie serwera dla kodu zarządzanego;
3) zapewnia spójne, zorientowane obiektowo środowisko programowania, niezależnie od tego, czy kod obiektu jest przechowywany i wykonywany lokalnie, wykonywany lokalnie, ale w sieci Web, czy wykonywany zdalnie;
4) Zapewniaj spójność dla deweloperów w różnych typach aplikacji, takich jak aplikacje oparte na systemie Windows i aplikacje oparte na sieci Web.

7. MS SQL

System równoważny do MS SQL musi spełniać następujące wymagania:

1) Posiada silnik baz danych który jest:
    a. odpowiedzialny jest za przetwarzanie zapytań,
    b. zarządza składowaniem, ochronie danych,

c. obsługuje niezbędne mechanizmy bezpieczeństwa, autoryzacji czy autentykacji.

2) Zawiera graficzny interfejs użytkownika , przeznaczony do administrowania, tworzenia baz, obiektów bazodanowychoraz do pisania i testowania skryptów, zapytań.

8. HTML

Język równoważny do HTML musi spełniać następujące wymagania:

1. musi umożliwiać realizację stron WWW,
2. opisywać stronę, a nie wygląd jej poszczególnych elementów,
3. posiada zdefiniowany pewien określony zestaw stylów, używanych na stronach WWW tj. nagłówki, akapity, listy, tabele,
4. posiada pewne elementy formatowania znaków, jak np. czcionka a każdy taki element posiada własną nazwę i występuje w formie znaczników lub tagów.

9. CSS

Język służący do opisu formy prezentacji (wyświetlania) stron WWW równoważny do CSS musi spełniać następujące wymagania:

1. umożliwić opis układu elementów na stronie WWW
2. umożliwić wybór koloru tekstu,
3. umożliwić wypełnienie tła,
4. wybrać rodzaj czcionki,
5. ustawić odstępy między elementami,
6. zdefiniować położenie jednego elementu względem drugiego.

10. Microsoft Certified Solutions Expert Server Infrastructure:

Za certyfikat równoważny do Microsoft Certified Solutions Expert Server Infrastructure Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Instalacja i konfiguracja serwerów;
2. Konfiguracja ról i funkcji serwera;
3. Konfiguracja funkcji Hyper-V;
4. Wdrażanie i konfiguracja podstawowych usług sieciowych;
5. Instalacja i administrowanie usługą Active Directory;
6. Tworzenie i zarządzanie zasadami grupy;
7. Wdrażanie i obsługa serwerów oraz zarządzanie nimi;
8. Konfiguracja usług plików i drukowania;
9. Konfiguracja usług sieciowych i dostępu;
10. Konfiguracja serwera zasad sieciowych (NPS);
11. Konfiguracja usługi Active Directory i zarządzanie nią;
12. Konfiguracja zasad grupy i zarządzanie nimi;
13. Konfiguracja wysokiej dostępności i zarządzanie nią;
14. Konfiguracja rozwiązań plików i pamięci masowej;
15. Implementowanie ciągłości biznesowej i odzyskiwania awaryjnego;
16. Konfiguracja usług sieciowych;
17. Konfiguracja infrastruktury usługi Active Directory;
18. Konfiguracja rozwiązań tożsamości i dostępu;

19. Planowanie i wdrażanie infrastruktury serwera;
20. Projektowanie i wdrażanie usług infrastruktury sieciowej;
21. Projektowanie i wdrażanie usług dostępu do sieci;
22. Projektowanie i wdrażanie infrastruktury usługi Active Directory (logicznej);
23. Projektowanie i wdrażanie infrastruktury usługi Active Directory (fizycznej);
24. Zarządzanie i obsługa infrastruktury serwera;
25. Planowanie i implementowanie infrastruktury przedsiębiorstwa o dużej dostępności;
26. Planowanie i implementowanie infrastruktury wirtualizacji serwera;
27. Projektowanie i wdrażanie rozwiązań tożsamości i dostępu;

11. Microsoft Certified Solutions Expert Private Cloud:

Za certyfikat równoważny do Microsoft Certified Solutions Expert Private Cloud Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Instalacja i konfiguracja serwerów;
2. Konfiguracja ról i funkcji serwera;
3. Konfiguracja funkcji Hyper-V;
4. Wdrażanie i konfiguracja podstawowych usług sieciowych;
5. Instalacja i administrowanie usługą Active Directory;
6. Tworzenie i zarządzanie zasadami grupy;
7. Wdrażanie i obsługa serwerów oraz zarządzanie nimi;
8. Konfiguracja usług plików i drukowania;
9. Konfiguracja usług sieciowych i dostępu;
10. Konfiguracja serwera zasad sieciowych (NPS);
11. Konfiguracja usługi Active Directory i zarządzanie nią;
12. Konfiguracja zasad grupy i zarządzanie nimi;
13. Konfiguracja wysokiej dostępności i zarządzanie nią;
14. Konfiguracja rozwiązań plików i pamięci masowej;
15. Implementowanie ciągłości biznesowej i odzyskiwania awaryjnego;
16. Konfiguracja usług sieciowych;
17. Konfiguracja infrastruktury usługi Active Directory;
18. Konfiguracja rozwiązań tożsamości i dostępu;
19. Konfigurowanie automatyzacji procesów centrum danych;
20. Wdrażanie monitorowania zasobów;
21. Monitorowanie zasobów;
22. Konfigurowanie i obsługa zarządzania usługami;
23. Zarządzanie konfiguracją i ochroną;
24. Projektowanie i wdrażanie programu System Center;
25. Konfigurowanie infrastruktury programu System Center;
26. Konfigurowanie sieci szkieletowej;
27. Konfigurowanie integracji programu System Center;
28. Konfigurowanie i wdrażanie maszyn wirtualnych oraz usług;

12. Microsoft Certified Solutions Expert: SharePoint:

Za certyfikat równoważny Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Planowanie instalacji;
2. Planowanie i konfigurowanie ustawień obejmujących całą farmę;
3. Tworzenie i konfigurowanie wyszukiwania przedsiębiorstwa;
4. Tworzenie i konfigurowanie aplikacji usługi zarządzanych metadanych;
5. Tworzenie i konfigurowanie aplikacji usługi profilów użytkowników;
6. Udostępnianie i konfigurowanie aplikacji sieci Web;
7. Tworzenie i obsługa zbiorów witryn;
8. Obsługa zabezpieczeń witryny i zbioru witryn;
9. Zarządzanie wyszukiwaniem;
10. Zarządzanie taksonomią;
11. Monitorowanie środowiska SharePoint;
12. Dostrajanie i optymalizowanie środowiska SharePoint;
13. Rozwiązywanie problemów ze środowiskiem SharePoint;
14. Planowanie obciążenia społecznościowego;
15. Planowanie i konfigurowanie obciążenia funkcji wyszukiwania;
16. Planowanie i konfigurowanie obciążenia funkcji zarządzania zawartością sieci Web;
17. Planowanie obciążenia funkcji zarządzania zawartością w organizacji;
18. Ocenianie zawartości i dostosowań;
19. Planowanie procesu uaktualniania;
20. Uaktualnianie zbioru witryn;

13. Microsoft Specialist Server Virtualization with Windows Server Hyper-V and System Center:

Za certyfikat równoważny do Microsoft Specialist Server Virtualization with Windows Server Hyper-V and System Center Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Konfiguracja funkcji Hyper-V;
2. Konfiguracja wysokiej dostępności maszyny wirtualnej i zarządzanie nią;
3. Wdrożenie infrastruktury wirtualizacji serwerów;
4. Monitorowanie i obsługa infrastruktury wirtualizacji serwera;

14. Microsoft Certified Solutions Associate: SQL Server 2012/2014 lub nowszy

Za certyfikat równoważny do Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Administracja bazami danych SQL Server
2. Tworzenie baz danych SQL Server
3. Zarzadzanie danymi za pomocą Transcat-SQL
4. Wykonywanie zapytań o dane za pomocą zaawansowanych komponentów Transact-SQL
5. Programowanie bazy danych przy użyciu języka Transact-SQL
6. Przeszukiwanie tabel przy użyciu sprzężeń
7. Wdrażanie funkcji i agregowanie danych
8. Modyfikacje danych
9. Grupowanie i przestawianie danych
10. Tworzenie obiektów
11. Wdrażanie obsługi błędów transakcji
12. Implementowanie typy danych i wartości NULL
13. Raportowanie danych
14. Zarzadzanie problemami
15. Wdrażanie hurtowni danych SQL Server

15. Microsoft Specialist Programing in HTML5 with JavaScript and CSS3:

Za certyfikat równoważny do Specialist Programing in HTML5 with JavaScript and CSS3 Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Znajomość i umiejętność tworzenia aplikacji przy użyciu HTML i CSS,
2. Tworzenie i dodawanie styli do stron HTML5,
   - tworzenie strony HTML5
   - stylizacja strony HTML5.
3. Znajomość języka JavaScript, w tym:
   - składnia JavaScript
   - programowanie HTML DOM z JavaScript,
   - jQuerry.
4. Tworzenie formularzy do zbierania i sprawdzania poprawności danych od użytkownika, w tym:
   - formatki i typy pól
   - sprawdzanie poprawności wprowadzania danych przez użytkownika za pomocą atrybutów HTML5
   - sprawdzanie poprawności wprowadzania danych przez użytkownika przy użyciu JavaScript
5. Komunikacja ze zdalnym źródłem danych
   - wysyłanie i odbieranie danych za pomocą XMLHTTP Request
   - wysyłanie i odbieranie danych za pomocą operacji AJAX jQuery
6. Stylizacja HTML5 za pomocą CSS3
7. Tworzenie obiektów i metod za pomocą JavaScript
   - pisanie dobrze ustrukturyzowanego JavaScript
   - tworzenie własnych obiektów
   - rozszerzanie obiektów
8. Tworzenie interaktywnych stron przy użyciu API HTML5
   - praca z plikami
   - dodawanie multimediów
   - reagowanie na lokalizację przeglądarki oraz kontekst
   - debugowanie i profilowanie aplikacji webowej
9. Dodanie nieaktywnego wsparcia do aplikacji sieciowych
   - odczytywanie i zapisywanie danych lokalnie
   - dodanie nieaktywnego wsparcia przy użyciu Application Cache
10. Wdrożenie adaptacyjnego interfejsu użytkownika.
11. Tworzenie zaawansowanej grafiki.
12. Animowanie interfejsu użytkownika
    - zastosowanie przejść CSS
    - przekształcanie elementów
    zastosowanie animacji CSS w oparciu o klatki kluczowe
13. Realizacja komunikacji w czasie rzeczywistym.
14. Tworzenie procesu Web Worker, wykonywanie przetwarzania asynchronicznego z wykorzystaniem Web Worker.

16. Microsoft Certified Solutions Associate Web Applications

Za certyfikat równoważny do Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Raportowanie o błędach
2. Tworzenie i obsługa rozwiązań problemów

3. Programowanie w HTML5 wraz z JavaScipt I CSS3
4. Tworzenie aplikacji internetowych w oparciu o ASP.NET MVC
5. Tworzenie rozwiązań Michrosoft Asure i usług internetowych
6. Tworzenie rozwiązań Michrosoft Sharepoint serwer
7. Administrowanie serwerem Microsoft Visual Studio Team Fundation Server
8. Implementacja obsługi błędów;
9. Monitorowanie
10. Analiza i rozwiazywanie błędów
11. Śledzenie aktywności;
12. Zarządzanie bezpieczeństwem;
13. Audyt dostępu do danych i szyfrowanie danych;
14. Obsługa bieżąca bazy danych;
15. Automatyzacja zarządzania
16. Aktualizacje danych
17. Konfiguracja
18. Wdrażanie rozwiązań
19. Udostępnianie i konfigurowanie aplikacji sieci Web
20. Debugowanie interakcji między klientem a usługą

17. Microsoft Certified Solutions Developer App Builder

Za certyfikat równoważny do Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Używanie programu Visual Studio 2017 do tworzenia i uruchamiania aplikacji sieci Web.
2. Tworzenie i stylizowanie stron w HTML5.
3. Dodawanie interaktywności do strony HTML5 za pomocą JavaScript.
4. Tworzenie formularzy HTML5 przy użyciu różnych typów danych wejściowych i weryfikacja danych wejściowych użytkownika za pomocą atrybutów HTML5 i kodu JavaScript.
5. Wysyłanie i odbieranie danych do i ze zdalnego źródła danych przy użyciu obiektów XMLHTTP Request i funkcji Fetch API.
6. Tworzenie styli stron HTML5 za pomocą CSS3.
7. Tworzenie dobrze zorganizowanego i łatwego w utrzymaniu kod JavaScript.
8. Pisanie nowoczesnego kodu JavaScript i używanie babel, aby był kompatybilny ze wszystkimi przeglądarkami.
9. Używanie typowych interfejsów API HTML5 w interaktywnych aplikacjach internetowych.
10. Tworzenie aplikacji internetowych obsługujących operacje w trybie offline.
11. Tworzenie stron internetowych w HTML5, które można dostosowywać do różnych urządzeń i formatów.
12. Dodawanie zaawansowanej grafiki do stron w HTML5, używając elementów Canvas oraz używając Scalable Vector Graphics.
13. Dodawanie animacji do strony w HTML5.
14. Używanie gniazd internetowych do wysyłania i odbierania danych między aplikacją internetową a serwerem.
15. Poprawianie szybkości reakcji aplikacji sieci Web, która wykonuje długotrwałe operacje, przy użyciu procesów Web Worker.
16. Używanie WebPack do pakowania aplikacji internetowych.
17. Projektowanie architektury i implementacja aplikacji internetowych, które będą spełniać zestaw wymagań funkcjonalnych, wymagań dotyczących interfejsu użytkownika i adresować modele biznesowe.
18. Tworzenie modeli MVC i pisanie kodu, który implementuje logikę biznesową w metodach, właściwościach i zdarzeniach modelu.
19. Dodawanie kontrolerów do aplikacji MVC, aby zarządzać interakcjami z użytkownikami, aktualizować modele oraz wybierać i zwracać widoki.
20. Tworzenie widoków w aplikacji MVC, która wyświetla i edytuje dane oraz współdziała z modelami i kontrolerami.

21. Uruchamianie testów jednostkowych i narzędzi do debugowania w aplikacji internetowej w programie Visual Studio i konfiguracja aplikacji do rozwiązywania problemów.
22. Tworzenie aplikacji internetowych, które używają silnika routingu ASP.NET, aby przedstawiać użytkownikom przyjazne adresy URL i logiczną hierarchię nawigacji.
23. Implementowanie spójnego wyglądu i styli, w tym znakowanie firmowe, w całej aplikacji internetowej MVC.
24. Używanie częściowych aktualizacji stron i pamięci podręcznej, aby zmniejszyć przepustowość sieci używaną przez aplikację i przyspieszenie odpowiedzi na żądania użytkowników.
25. Pisanie kodu JavaScript, który działa po stronie klienta i wykorzystuje bibliotekę skryptów jQuery do optymalizacji czasu reakcji aplikacji internetowej MVC.
26. Zaimplementuj pełnego systemu rejestracji w aplikacji internetowej MVC.
27. Budowanie aplikacji MVC, która jest odporna na złośliwe ataki i przechowuje informacje o użytkownikach i preferencjach.
28. Konfiguracja usługi internetową Microsoft Azure i wywoływanie jej z poziomu aplikacji MVC.
29. Modyfikowanie sposobu obsługi żądań przeglądarki przez aplikację MVC.
30. Wdrażanie aplikacji internetowej ASP.NET MVC z komputera deweloperskiego na serwer sieci Web,
31. Projektowanie i opracowywanie aplikacji skoncentrowanych na danych przy użyciu programu Visual Studio 2017 i Entity Framework Core.
32. Projektowanie, implementowanie i używanie usług HTTP przy użyciu ASP.NET Core.
33. Rozszerzanie usług HTTP przy użyciu ASP.NET Core.
34. Hostowanie usługi lokalnie i na platformie Microsoft Azure.
35. Wdrażanie usług zarówno w środowiskach lokalnych, jak i chmurowych oraz zarządzaj interfejsem i zasadami ich usług.
36. Przechowywanie danych, buforowanie, dystrybuowanie i synchronizacja danych.
37. Monitorowanie, rejestrowanie i rozwiązywanie problemów z usługami.
38. Opisywanie koncepcji i standardów tożsamości opartych na oświadczeniach oraz wdrażanie uwierzytelniania i autoryzacji za pomocą usługi Azure Active Directory.
39. Tworzenie skalowalnych aplikacji usługowych.

18. Microsoft Certified Solutions Expert: Data Management and Analytics

Za certyfikat równoważny do Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Uwierzytelnianie i autoryzacja użytkowników,
2. Przypisywanie ról serwera i bazy danych,
3. Zezwalanie użytkownikom na dostęp do zasobów,
4. Ochrona danych za pomocą szyfrowania,
5. Tworzenie modeli odzyskiwania i strategii tworzenia kopii zapasowych,
6. Tworzenie kopii zapasowych baz danych SQL Server,
7. Przywracanie bazy danych programu SQL Server,
8. Zautomatyzowanie zarządzania bazą danych,
9. Konfigurowanie zabezpieczeń dla agenta SQL Server,
10. Zarządzanie alertami i powiadomieniami,
11. Zarządzanie programem SQL Server za pomocą PowerShell,
12. Śledzenie dostępu do SQL Server,
13. Monitorowanie infrastruktury SQL Server,
14. Rozwiązywanie problemów z infrastrukturą SQL Server,
15. Importowanie i eksportowanie danych,
16. Udostępnianie serwera bazy danych,
17. Uaktualnianie SQL Server,
18. Konfigurowanie SQL Server,
19. Zarządzanie bazami danych i plikami (współdzielone),
20. Tworzenie, migrowanie i zarządzanie bazami danych w chmurze
21. Tworzenie instrukcję SELECT dla pojedynczej tabeli, obejmującą wiele tabel, z filtrowaniem i sortowaniem,
22. Pisania instrukcji DML,
23. Pisania zapytań, które używają wbudowanych funkcji,
24. Pisanie zapytań, które agregują dane
25. Pisanie podzapytań
26. Tworzenie i implementacja widoków oraz funkcji przedstawianych w tabeli,
27. Używanie operatorów zestawów, aby połączyć wyniki zapytania,
28. Pisanie zapytań, które używają funkcji rankingu okien, przesunięcia i agregacj,i przekształcanie danych, implementując pivot, unpivot, rollup i cube,
29. Tworzenie i wdrażanie procedur składowanych,
30. Dodawanie konstrukcji programistycznych, takich jak zmienne, warunki i pętle do kodu T-SQL
31. Tworzenie zaawansowanych projektów tabel,
32. Zapewnienie integralności danych dzięki ograniczeniom,
33. Tworzenie indeksów, w tym indeksów zoptymalizowanych i indeksy magazynu kolumn,
34. Projektowanie i wdrażanie widoków,
35. Projektowanie i implementowanie procedur składowanych
36. Projektowanie i wdrażanie funkcji zdefiniowanych przez użytkownika,
37. Reagowanie na manipulację danymi za pomocą wyzwalaczy,
38. Projektowanie i wdrażanie tabel w pamięci,
39. Implementowanie kodu zarządzanego w programie SQL Server,
40. Przechowywanie i wysyłanie zapytań do danych XML,
41. Praca z danymi przestrzennymi,
42. Przechowywanie i wysyłanie zapytań do obiektów blob i dokumentów tekstowych.

19. Microsoft Certified Solutions Developer SharePoint Applications

Za certyfikat równoważny do Zamawiający uzna certyfikat potwierdzający poniższe umiejętności:

1. Projektowanie funkcji i rozwiązań oraz zarządzanie nimi,
2. Opracowywanie kodu dla niestandardowych składników po stronie serwera,
3. Zarządzanie uwierzytelnianiem i autoryzacją oraz dostosowywanie ich,
4. Tworzenie niestandardowych witryn i list oraz zarządzanie cyklem życia witryn.
5. Możliwość tworzenia i projektowania aplikacji SharePoint,
6. Używanie modelu obiektów po stronie klienta i interfejsu API REST,
7. Opisywanie aplikacji dla platformy programistycznej SharePoint,
8. Używanie modeli obiektów po stronie klienta i interfejsu API REST do komunikacji z SharePoint,
9. Konfigurowanie zabezpieczeń aplikacji dla SharePoint,
10. optymalizowanie wydajności aplikacji dla SharePoint,
11. Tworzenie i stosowanie zarządzanych metadanych w programie SharePoint 2013.

W sytuacji, gdy na rynku istnieje wiele rodzajów uznawanych certyfikatów potwierdzających jakość świadczonych usług będących przedmiotem zamówienia, wydawanych przez odpowiednie podmioty, Zamawiający dopuszcza rozwiązania równoważne opisane poniżej. Zamawiający wskazuje konkretny certyfikat, niemniej z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do ich wydawania, o którym mowa poniżej w zakresie świadczenia usług będących przedmiotem zamówienia.

Za rozwiązanie równoważne do wskazanych wyżej rozwiązań opartych wykorzystywanej przez Zamawiającego technologii Microsoft, w tym Microsoft Hyper-V, SharePoint, System Center, innych jak również w przypadku certyfikatów potwierdzających wiedzę w powyższym zakresie, Zamawiający uznaje rozwiązania spełniające wymagania opisane w Załączniku– Warunki równoważności dotyczące znaków towarowych

W przypadku pozostałych pojęć oraz certyfikatów, niewymienionych w Załączniku Warunki równoważności dotyczące znaków towarowych, poprzez pojęcie „certyfikat równoważny" Zamawiający rozumie, iż Wykonawca dla danej roli przedstawi certyfikat, który: jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy dla danej roli, co jest rozumiane jako: analogiczna dziedzina merytoryczna wynikająca z wiedzy, której dotyczy certyfikat (np. zarządzenie bazami danych, kompetencje związane z zarządzaniem projektami, testowaniem, administracją bazami danych, programowanie, itp.); analogiczny stopień poziomu kompetencji (np. podstawowy, zaawansowany, ekspert); analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu (np.: konieczność wykazania się uczestnictwem w określonej liczbie projektów w danej roli, itp.); uzyskanie certyfikatu potwierdzone jest egzaminem (jeżeli uzyskanie wskazanego certyfikatu wymaga egzaminu). Obowiązek wykazania, iż zaproponowane przez Wykonawcę osoby posiadają wiedzę/umiejętności/certyfikaty równoważne do rozwiązań wskazanych przez Zamawiającego, spoczywa na Wykonawcy.