Specyfikacja dotycząca oprogramowania

I. Wymagania dla „profesjonalny system operacyjny w wersji 64 bitowej” 2
II. Wymagania dla „pakietu biurowego” 3
III. Wymagania dla „programu antywirusowego” 6
IV. Wymagania dla „standardowego serwerowego systemu operacyjnego” 7
V. Wymagania dla „zestawu programów branżowych” 20
RÓWNOWAŻNOŚĆ 23

I. Wymagania dla „profesjonalny system operacyjny w wersji 64 bitowej"

System musi posiadać następujące, wbudowane cechy:
1) Funkcjonalne:

- Polska wersja językowa.
- Możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Office 2010 oraz systemu domenowego MS Windows (Windows Server 2003).
- Dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek.
- Możliwość zdalnej, automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
- Możliwość automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości przez sieć komputerową.
- Możliwość wdrożenia nowego obrazu przez zdalną instalację.
- Graficzne środowisko instalacji i konfiguracji w języku polskim.
- Możliwość udostępniania i przejmowania pulpitu zdalnego.
- Możliwość udostępniania plików i drukarek.
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk sprzętowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
- Zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń sieciowych, standardów USB, urządzeń Plug & Play, WiFi).
- Wyposażenie systemu w zintegrowaną zaporę sieciową wraz z konsolą do zarządzania ustawieniami i regułami IP v4 i v6.
- Zapewnienie pełnej kompatybilności z oferowanym sprzętem.
- Zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim.
- Zintegrowanie z systemem modułu wyszukiwania informacji.
- Możliwość wykonania kopii bezpieczeństwa (całego dysku, wybranych folderów, kopii przyrostowych) wraz z możliwością automatycznego odzyskania wersji wcześniejszej.
- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacja dostępna u producenta nieodpłatnie bez ograniczeń czasowych.
- Dodatkowo system równoważny musi zapewniać obsługę podpisu elektronicznego (certyfikat kwalifikowany).
- Zamawiający dopuszcza zaoferowanie równoważnych systemów operacyjnych, które muszą akceptować te same kody binarne aplikacji i posiadać co najmniej taką samą funkcjonalność.
- Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji.
- Do komputera powinno zostać dołączone oprogramowanie producenta komputera umożliwiające tworzenie obrazów oraz ułatwia zarządzanie sprzętem, systemem BIOS i zabezpieczeniami.
- Możliwość instalacji na urządzeniach w placówkach edukacyjnych kształcenia zawodowego i ustawicznego.

Przykładowe oprogramowanie spełniające te wymagania to Microsoft Windows 10 Professional PL

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*Na stanowisko*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja/Administracja (w zależności od miejsca dostawy)*
Nośnik	*Partycja Recovery, z możliwością przywracania systemu do stanu fabrycznego.*

II. Wymagania dla „pakietu biurowego"

Program musi spełniać wymagania poprzez wbudowane mechanizmy bez użycia dodatkowych aplikacji oraz musi posiadać następujące wbudowane cechy:

1) Funkcjonalne:

1. Licencja na oprogramowanie musi pozwalać na dowolne przenoszenie oprogramowania niezależnie od sprzętu oraz umożliwiać instalację z wykorzystaniem jednego klucza (jeżeli występuje).
2. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi (np. w przypadku wymiany stacji roboczej).
3. Licencjonowanie musi uwzględniać prawo do (w okresie przynajmniej 5 lat) bezpłatnej instalacji udostępnianych przez producenta uaktualnień i poprawek krytycznych i opcjonalnych.
4. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej licencje pochodzące od jednego producenta, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.
5. Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji zamawianego oprogramowania i korzystania z kopii zamiennych (możliwość kopiowanie oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.
6. Wymagania zawarte w specyfikacjach technicznych poszczególnych produktów odnoszą się do natywnej funkcjonalności oferowanego oprogramowania bez użycia dodatkowego oprogramowania, chyba, że wymóg szczegółowy stanowi inaczej.
7. 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.
8. Wymagania odnośnie interfejsu użytkownika:
   a) Możliwość instalacji w postaci zwirtualizowanej aplikacji dostarczanej sieciowo na stację klienta.
   b) Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi Active Directory.
   c) Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.

9. 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 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 wykorzystanie schematów XML,
   d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,
10. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
11. Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
12. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
13. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
14. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji
   d) Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
15. 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) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   k) Określenie układu strony (pionowa/pozioma).
   l) Wydruk dokumentów.
   m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego I z narzędzia do zarządzania informacją prywatną.
   n) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007, 2010, 2013 oraz 2016. Z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
   o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
   p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym Prawem.
   q) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego Zgodnie z wymaganiami obowiązującego w Polsce prawa.
16. Arkusz kalkulacyjny musi umożliwiać:
   a) Tworzenie raportów tabelarycznych
   b) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych

c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach Czasu.
d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, Pliki tekstowe, pliki XML, webservice)
e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające Analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów Bazujących na danych z tabeli przestawnych
g) Wyszukiwanie i zamianę danych
h) Wykonywanie analiz danych przy użyciu formatowania warunkowego
i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
k) Formatowanie czasu, daty i wartości finansowych z polskim formatem
l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
m) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007, 2010, 2013 oraz 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji Specjalnych i makropoleceń..
n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

17. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a) Przygotowywanie prezentacji multimedialnych, które będą:
b) Prezentowanie przy użyciu projektora multimedialnego
c) Drukowanie w formacie umożliwiającym robienie notatek
d) Zapisanie jako prezentacja tylko do odczytu.
e) Nagrywanie narracji i dołączanie jej do prezentacji
f) Opatrywanie slajdów notatkami dla prezentera
g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j) Możliwość tworzenia animacji obiektów i całych slajdów
k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, A na drugim widoczne są slajdy i notatki prezentera
l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, 2010, 2013 oraz 2016.

18. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
d) Automatyczne grupowanie poczty o tym samym tytule
e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
g) Zarządzanie kalendarzem
h) Udostępnianie kalendarza innym użytkownikom
i) Przeglądanie kalendarza innych użytkowników
j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
k) Zarządzanie listą zadań
l) Zlecanie zadań innym użytkownikom
m) Zarządzanie listą kontaktów

n) Udostępnianie listy kontaktów innym użytkownikom
o) Przeglądanie listy kontaktów innych użytkowników
p) Możliwość przesyłania kontaktów innym użytkowników.

19. Możliwość instalacji na urządzeniach w placówkach edukacyjnych kształcenia zawodowego i ustawicznego.

Przykładowe oprogramowanie spełniające te wymagania to MS Office 2019 wersja Professional

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*Na stanowisko*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja/Administracja (w zależności od miejsca dostawy)*

III. Wymagania dla „programu antywirusowego"

Program musi spełniać wymagania poprzez wbudowane mechanizmy bez użycia dodatkowych aplikacji oraz musi posiadać następujące wbudowane cechy:

1) Funkcjonalne:

- Polska wersja językowa,
- możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez zamawiającego licencji Microsoft Office 2010 oraz systemu domenowego MS Windows (Windows Server 2003),
- dostępność do aktualnych baz sygnatur wirusów oraz komponentów programu
- moduł śledzenia o ostrzegania przed najnowszymi zagrożeniami.
- przesyłanie strumieniowe w czasie rzeczywistym informacji dotyczących zagrożeń,
- wsparcie laboratorium w zakresie aktualności zabezpieczeń,
- możliwość sprawdzenia reputacji procesów i plików bezpośrednio z poziomu interfejsu programu lub menu kontekstowego,
- nieobciążanie systemu w trakcie działania,
- możliwość monitorowania użycia kamery internetowej podłączonej do urządzenia,
- informowanie użytkownika o próbie użycia kamery przez inne aplikacje,
- możliwość aktywacji funkcji skanowania wewnętrznej sieci Użytkownika w celu wykrycia urządzeń nieautoryzowanych do jej używania,
- możliwość wykonania audytu routera do którego podłączony jest komputer użytkownika,
- wbudowany moduł zapory osobistej z systemem IDS,
- wbudowany moduł kontroli przeglądanych stron internetowych,
- możliwość ochrony dedykowanej dla bankowości elektronicznej,
- zwiększając zabezpieczenie operacji,
- wsparcie techniczne prowadzone w języku polskim.

2) Systemowe:

- operacyjność w systemach komputerowych z systemami operacyjnymi Windows 7, 8, 10
- obsługiwane procesory architektury x86-x64

3) Licencja wieczysta do korzystania w szkołach i uczelniach. Aktualizacja Bazy wirusów na min. 24 miesiące.

Przykładowe oprogramowanie spełniające te wymagania to ESET Internet Security

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*Na urządzenie*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja/Administracja (w zależności od miejsca dostawy)*

IV. Wymagania dla „standardowego serwerowego systemu operacyjnego"

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 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: Login i hasło, Karty z certyfikatami (smartcard), 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:
   - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
   - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
   - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
   - 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:
   - Dystrybucję certyfikatów poprzez http
   - Konsolidację CA dla wielu lasów domeny,
   - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   - 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:
   - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   - Obsługi 4-KB sektorów dysków
   - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   - 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.

Elementy zarządzania

1. Zarządzanie serwerem 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*

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,
- Bazy Operacyjnej przechowującej informacje o zarządzanych elementach,
- 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.
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.
W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.
a) Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp...

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

System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.
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)

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

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
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
a. 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

1) Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:
a) Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
b) Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:

- profilu sprzętowego
- profilu systemu operacyjnego,
- przygotowanych dysków twardych,

2) Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.
3) 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

4) System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.
5) 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.
6) 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.
7) System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
8) 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 kopii zapasowych musi posiadać następujące cechy:
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:
- na puli magazynowej złożonej z dysków twardych
- na napędach I bibliotekach taśmowych
- 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:
- Krótkoterminowe: Pule dyskowe – do 448 dni
- Online: Zasoby chmurowe – do 3360 dni
- Krótkoterminowe: Taśmy – do 12 tygodni
- 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:
- lokalizacji oryginalnej
- lokalizacji alternatywnej
- 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:
- System operacyjny Windows (w tym pliki, system state i BMR)
- Maszyny wirtualne na platformie Hyper-V
- Bazy danych MS SQL
- Sharepoint
- 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:

- System.
- Planowanie.
- Monitorowanie.
- Zarządzanie plikami.
- E-mail.
- Powiadomienia.
- Narzędzia.
- Zarządzanie plikami tekstowymi.
- Kontrola przepływów (runbooks).

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:

- Active Directory
- Exchange Admin
- Exchange Users
- FTP Integration
- HP iLO and OA
- HP Operations Manager
- HP Service Manager

- IBM Tivoli Netcool/OMNIbus
- Representational State Transfer (REST)
- Sharepoint
- Microsoft Azure
- VMware vSphere
- 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:

- Definicje przebiegów procesów
- Stan uruchomionych przebiegów
- Informacje statusowe (logs)
- 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:

- Zarządzanie incydentami
- Zarządzanie problemami
- Zarządzanie zmianą
- Zarządzanie

b) W zakresie zarządzania incydentami i problemami system powinien posiadać przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia.
3. Komponent CMDB:
a) Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym: Użytkownik – Komputer.
b) System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:

- Konektor do systemu zarządzania infrastrukturą i oprogramowaniem
- Konektor do systemu zarządzania komponentami
- Konektor do systemu zarządzania środowiskami wirtualnym
- Konektor do systemu automatyzacji zarządzania środowisk IT
- 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:
   - 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,
8. 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.
System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

Przykładowe oprogramowanie spełniające te wymagania to Microsoft Windows Server Standard 2019 2 Core MOLP EDU

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*MOLP*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja*

V. Wymagania dla „zestawu programów branżowych"

Wymagania dla „programu do kosztorysowania":

Program musi posiadać następujące, wbudowane cechy:
1) Funkcjonalne:
- Polska wersja językowa,
- możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Windows 10 oraz systemu domenowego MS Windows (Windows Server 2003),
- dostęp do baz katalogów typu min.: KNR, KNNR, KNR-W, TZKNBK (PKZ), KNP,
- możliwość współpracy z dostępnymi bazami cenowymi,
- możliwość zapisu kosztorysu w standardzie xml,
- możliwość integracji procesu kosztorysowania z różnymi systemami zarządzania firmą,
- tworzenie kosztorysów zgodnie z normami obowiązującymi w Polsce i UE (procedury FIDIC),
- współpraca z programami do planowania i harmonogramowania,
- możliwość pracy w sieci komputerowej,
- tworzenie kosztorysów zawierających warianty na poziomie działów, pozycji lub elementów RMS,
- funkcja rejestracji zmian wraz z możliwością akceptacji i cofnięcia zmian,
- możliwość tworzenia kosztorysów wariantowych, złożonych, kosztorysów z wykazem różnic,
- możliwość dynamicznej pracy na kilku kosztorysach jednocześnie,
- całkowicie dowolne definiowanie sposobu liczenia narzutów,
- wyliczanie nakładów metodą interpolacji i ekstrapolacji,
- rozliczenia robót tymczasowych w innych pozycjach,
- zapisywanie kosztorysu i jego działów w cenniku obiektów,
- automatyczne wyliczanie nakładów dodatkowych (np. koszty jednostkowe transportu),
- korzystanie z biblioteki wzorów i funkcji matematycznych,
- import danych obmiarowych z innych programów,
- mechanizm kluczy wykonawczych i lokalizacyjnych, ułatwiający współpracę z harmonogramami,
- rozliczanie wykonanych robót,
- możliwość wprowadzanie kodów CPV,
- import/eksport do/z plików typu PDF,
- komunikacja przez Internet z bazą intercenbud.pl,
- współpraca z innymi bazami, m.in. tj. orgbud, bistyp, sekocenbud,
- możliwość tworzenia własnych cenników.

2) Systemowe:

- Praca na komputerach o minimalnych parametrach:
  Windows 10, Windows 8.1, Windows 7 SP1 64 bitowe
  Procesor minimum 500MHz
  Pamięć RAM min. 512 MB
  Grafika: 1024x768 min.
  Połączenie z Internetem.

3) Licencja edukacyjna do korzystania w szkołach i uczelniach o profilu technicznym związanym z budownictwem, architekturą – na 16 stanowisk

Przykładowe oprogramowanie spełniające te wymagania to Norma PRO.

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*zbiorcza*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja*

Wymagania dla „profesjonalnego programu do projektowania ogrodów"

Program musi posiadać następujące, wbudowane cechy:
1) Funkcjonalne:
- Możliwość renderingu oraz płynną wizualizacje 3D,
- Możliwość definiowania ustawień arkusza, projektu oraz obszaru projektowania (bez ograniczeń formatu) w zakresie: wielkości, skali, siatki, przezroczystości,
- Projektowanie koncepcyjne w rzucie 2D,
- Rozbudowany panel narzędzi rysowania i edycji,
- Możliwość importowania plików 2D: min. JPG, GIF, PNG,
- Możliwość Importu plików 3D,
- Możliwość ustawienia trybów widoków trójwymiarowych: w aksonometrii lub perspektywie,
- Wirtualny spacer po ogrodzie,
- Przekroje widokowe, projekt techniczny oraz wymiarowanie,
- Możliwość wyeksportowania użytych w projekcie materiałów do pliku CSV,
- Możliwość tworzenia własnych nazw i symboli,
- Możliwość modelowania ukształtowania terenu,
- Biblioteka zawierająca min. 8000 pozycji,
- Katalog biblioteki według: wg min. 3 parametrów,
- Symulacja kalendarza biodynamicznego roślin użytych w projekcie,
- Symulacja rzutów cienia w zależności od pory dnia,
- Możliwość zmiany wyglądu w zależności od pory roku,
- Możliwość rozbudowy programu o dodatkowe moduły zewnętrznych baz producentów,
- Automatyczna aktualizacja programu i bazy danych przez Internet,
- praca w trybie ONLINE I OFFLINE,
- Polska wersja językowa.
- instrukcja użytkownika w języku polskim.

2) Systemowe:
- Praca na komputerach o minimalnych parametrach:
  Procesor dwu- lub cztero- rdzeniowy 2,0 GHz
  System operacyjny Windows 7, 8, 10 i Mac OS X, 64 bitowe
  Pamięć RAM min. 4 GB
  Karta graficzna min. 2 GB RAM

Rozdzielczość: min. 1366x 768 px

3) Licencja edukacyjna do korzystania w szkołach i uczelniach o profilu technicznym związanym z budownictwem, architekturą – na 13 stanowisk

Przykładowe oprogramowanie spełniające te wymagania to Gardenphilia DESIGNER 2019.

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*zbiorcza*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja*

Wymagania dla „programu do ewidencji gruntów"

Program musi posiadać następujące, wbudowane cechy:
1) Funkcjonalne:
- możliwość zakładania oraz prowadzenia ewidencji gruntów, budynków i lokali zgodnie z obowiązującymi przepisami prawa,
- prowadzenie ewidencji podmiotów w podziale na minimum cztery kryteria, w tym obowiązkowo na kryteria: osoby fizyczne, instytucje, małżeństwa, podmioty grupowe,
- prowadzenie ewidencji podmiotów w podziale na przedmiot ewidencji (działek, budynków, lokali),
- obsługa jednostek rejestrowych (gruntowych, budynkowych i lokalowych),
- import i eksport danych do formatów *.gml,

2) Systemowe:
praca w systemie operacyjnym: Windows 7, 8, 10 i Mac OS X, 64 bitowe

3) Licencja edukacyjna do korzystania w szkołach i uczelniach o profilu technicznym związanym z budownictwem, architekturą – na 16 stanowisk

Przykładowe oprogramowanie spełniające te wymagania to EWOPIS.

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*zbiorcza*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja*

Wymagania dla „programu do prowadzenia numerycznej mapy zasadniczej"

Program musi posiadać następujące, wbudowane cechy:
1) Funkcjonalne:
- możliwość tworzenia i prowadzenia numerycznej mapy zasadniczej zgodny z obowiązującymi przepisami prawa,
- zgodność ze standardami technicznymi wykonywania geodezyjnych pomiarów sytuacyjnych i wysokościowych,
- zgodność z wytycznymi dla map zasadniczych, GESUT, BDOT500,
- zgodność z wytycznymi dla ewidencji gruntów i budynków.
- możliwość prowadzenia danych stanowiących infrastrukturę informacji przestrzennej funkcjonującej w Polsce,
- możliwość prowadzenia graficznej bazy danych oraz powiązanie jej z danymi opisowymi (w postaci zintegrowanej tabeli lub zewnętrznej bazy danych),
- możliwość wykonywania analiz przestrzennych, będąc tym samym podstawą Systemu Informacji o Terenie,

- wymiana danych (eksport i import) z wykorzystaniem różnych formatów, w tym m.in.: *.gml, *.dxf, *.shp, itp.

2) Systemowe:
praca w systemie operacyjnym: Windows 7, 8, 10 i Mac OS X, 64 bitowe

3) Licencja edukacyjna do korzystania w szkołach i uczelniach o profilu technicznym związanym z budownictwem, architekturą – na 16 stanowisk

Przykładowe oprogramowanie spełniające te wymagania to EWMAPA.

Wersja językowa	*Polska wersja językowa interfejsu użytkownika*
Sposób licencjonowania	*zbiorcza*
Okres licencji	*Wieczysta*
Wykorzystanie licencji	*Edukacja*

RÓWNOWAŻNOŚĆ

Informacje dla Wykonawcy:
- Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego.
- Oprogramowanie równoważne musi być kompatybilne z wymienionym typem oprogramowania oraz posiadać wszystkie jego cechy funkcjonalne.
- musi charakteryzować się cechami oprogramowania równoważnego
- musi spełniać warunki opisane w punkcie Kryteria równoważności

Kryteria równoważności – ocena, zasady, wymagania, budowanie kompetencji
1) We wszystkich miejscach niniejszego dokumentu, w których użyto przykładowego znaku towarowego, patentu lub pochodzenia, jest to uzasadnione specyfiką przedmiotu zamówienia i Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń.
2) Wykonawca, który powoła się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowany przez niego przedmiot dostawy spełnia wymagania określone przez Zamawiającego.
3) Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanych rozwiązań z rozwiązaniami opisanymi poprzez wskazanie przykładowego znaku towarowego, patentu lub pochodzenia, spoczywa na Wykonawcy, składającym ofertę równoważną.
4) Zamawiający wymaga, aby zaoferowane przez Wykonawcę rozwiązania równoważne nie wiązały się z koniecznością wykonania dodatkowych prac integracyjnych, testowych czy migracyjnych po stronie Zamawiającego, tym samym poniesienia dodatkowych, niezaplanowanych kosztów. Przedmiotem zamówienia jest modernizacja wykorzystywanych serwerów infrastruktury Państwa, w związku z powyższym Zamawiający nie dopuszcza rozwiązań, które powodowałyby konieczność przeprowadzania testów migracji czy wykonywania jakichkolwiek prac dodatkowych.
5) W celu potwierdzenia, iż oferowana dostawa spełnia wymagania określone przez Zamawiającego Wykonawca, który zaoferuje oprogramowanie równoważne do wskazanego przez Zamawiającego załączy do oferty szczegółową specyfikację techniczną dla każdego rodzaju oferowanego oprogramowania równoważnego z osobna, wystawioną przez producenta każdego rodzaju oferowanego oprogramowania równoważnego, zawierającą opis wszystkich cech i funkcjonalności oferowanego oprogramowania równoważnego.
6) Zaoferowane rozwiązanie równoważne musi być w pełni kompatybilne z istniejącymi rozwiązaniami w środowisku, w tym dedykowanymi ze względu na specyfikę aplikacjami, systemami, także w warstwie aplikacyjnej.
7) Zamawiający przygotuje środowisko testowe i scenariusze testowe w celach udowodnienia przez Wykonawcę spełnienia warunków równoważności. Koszty związane z przeprowadzenia jakichkolwiek

prac związanych z wykonywaniem testów i przygotowaniem środowiska testowego w tym instalacji, konfiguracji i integracji dostarczonego produktu z systemami Zamawiającego, przy uwzględnieniu m.in. licencji, konsultacji specjalistów, przygotowania scenariuszy testowych, szkoleń ponosi w całości Wykonawca.

8) W przypadku zaoferowania przez Wykonawcę rozwiązań równoważnych w zakresie systemów operacyjnych, rozwiązań wirtualizacji, platformy aplikacyjnej, gdzie integracja i zgodność z istniejącymi aplikacjami jest kluczowa, Zamawiający ze względu na przeprowadzaną modernizację istniejących środowisk infrastruktury Państwa nie dopuszcza rozwiązań, które powodowałyby konieczność wykonywania dodatkowych prac związanych z migracją, ponieważ specyfika i konfiguracja oprogramowania jest w pełni przetestowana, w tym przeprowadzony został tuning systemów i aplikacji.
9) Wykonawca musi zapewnić oraz udowodnić spełnienie określonych warunków.
10) Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.
11) Integracja dostarczonego równoważnego oprogramowania nie może wymuszać wykonania dodatkowych zmian programistycznych po stronie posiadanego przez Zamawiającego oprogramowania oraz musi umożliwiać integrację ze wszystkimi rozwiązaniami, które Zamawiający posiada w ramach istniejących środowisk. Wykonawca oddeleguje zespół posiadający ww. wymagania kompetencyjne oraz poświadczenia w celu przeprowadzenia migracji istniejących środowisk produkcyjnych. W przypadku wystąpienia jakichkolwiek trudności, które skutkować będą niepoprawną pracą bądź przerwami w ciągłości działania systemów i usług, na Wykonawcę mogą zostać przeniesione w całości wszelkie kary oraz zobowiązania, którymi Zamawiający zostanie obciążony.
12) Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu, licencji czasowej, OEM, z wyłączeniem, w którym Zamawiający określił taki warunek w opisie oprogramowania.
13) Licencje muszą pochodzić z autoryzowanego kanału dystrybucji.
14) Zamawiający nie dopuszcza zaoferowania oprogramowania i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu, z wyłączeniem, w którym Zamawiający określił taki warunek w opisie oprogramowania.
15) Oprogramowanie musi zostać dostarczone w najnowszej dostępnej wersji wydanej przez producenta oprogramowania, z wyłączeniem, w której Zamawiający określił taki warunek w opisie oprogramowania.
16) W przypadku zaoferowania przez Wykonawcę rozwiązań równoważnych, Wykonawca na swój koszt przeprowadzi szkolenia dla administratorów i użytkowników wskazanych przez Zamawiającego.
17) Dedykowane szkolenie w zależności od grupy docelowej będzie trwało min. 2 dni i będzie miało charakter warsztatowy, praktyczny. Liczba uczestników każdego ze szkoleń wynosi min. 10 osób.
18) Szkolenie dla administratorów ma na celu pozyskanie kompetencji w zakresie administrowania dostarczonymi rozwiązaniami m.in. zarządzania użytkownikami, dostępami, zmian w konfiguracji, modyfikacji, integracji z zainstalowanymi rozwiązaniami w środowisku Zamawiającego.
19) Szkolenie dla użytkowników ma na celu przećwiczenia funkcji oprogramowania, scenariuszy użycia.
20) Wykonawca przedstawi do akceptacji plan i zakres szkolenia dla obu grup wraz z terminem.
21) Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 5 minut.
22) Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ.

Zastępca Dyrektora Departamentu
Iwona Gnyp

Koordynator Projektu
mgr Łukasz Dziaduk