i. Krótkoterminowe: Pule dyskowe – do 448 dni

ii. Online: Zasoby chmurowe – do 3360 dni

iii. Krótkoterminowe: Taśmy – do 12 tygodni

iv. Długoterminowe: Taśmy – do 99 lat

3. Odzyskiwanie danych:

   a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje"

   b. System kopii zapasowych musi umożliwiać odtworzenie danych do:

      i. lokalizacji oryginalnej

      ii. lokalizacji alternatywnej

      iii. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych

4. Agent kopii zapasowej

   a. Agent powinien posiadać możliwość współpracy z komponentami VSC.

   b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych" oraz wykorzystywanego pasma w i poza godzinami „biznesowymi"

   c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:

      i. System operacyjny Windows (w tym pliki, system state i BMR)

      ii. Maszyny wirtualne na platformie Hyper-V

      iii. Bazy danych MS SQL

      iv. Sharepoint

5. Konsola administracyjna:

   a. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach

   b. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów

   c. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń

   d. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych

   e. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych

f. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).

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

1. Architektura:

    a. System musi posiadać graficzną konsolę dla administratorów (autorów) pozwalającą w łatwy sposób (bez znajomości języków programowania) tworzenie przebiegów procesów (runbooks) przy pomocy gotowych elementów aktywności.

    b. System musi posiadać tester przebiegów pozwalający na sprawdzenie poprawności wykonywania stworzonego przez administratora (autora) pokazując informacje o wykonaniu poszczególnych kroków, informacje wchodzące i wychodzące z poszczególnych kroków, możliwość ustawiania pułapek (breakpoints) oraz wykonywania krok po kroku.

    c. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.

    d. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).

    e. System powinien posiadać konsolę webową pozwalającą na podgląd zdefiniowanych przebiegów procesów, ich stanu, informacji historycznych o wykonanych przebiegach oraz pozwalająca na uruchamianie przebiegów procesów na żądanie.

    f. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).

2. Tworzenie przebiegów:

    a. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.

    b. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.

    c. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:

        i. System:

            1. Run Program
            2. Run .Net Script
            3. End Process
            4. Start/Stop Service
            5. Restart System
            6. Save Event Log

7. implementacji CIM Query
8. Run SSH Command
9. Get SNMP Variable
10. Monitor SNMP Trap
11. Send SNMP Trap
12. Set SNMP Variable

ii. Planowanie:

1. Monitor Date/Time
2. Check Schedule

iii. Monitorowanie:

1. Monitor Event Log
2. Monitor Service
3. Get Service Status
4. Monitor Process
5. Get Process Status
6. Monitor Computer/IP Status
7. Monitor Disk Space
8. Get Disk Space Status
9. Monitor Internet Application
10. Get Internet Application Status
11. pozostałych komponentów sprzętowych serwera

iv. Zarządzanie plikami:

1. Compress File
2. Copy File
3. Create Folder
4. Decompress File
5. Delete File
6. Delete Folder
7. Get File Status
8. Monitor File
9. Monitor Folder
10. Move File

11. Move Folder
12. PGP Decrypt File
13. PGP Encrypt File
14. Print File
15. Rename File

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

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

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

viii. Zarządzanie plikami tekstowymi:
    1. Append Line

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

ix. Kontrola przepływów (runbooks):

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

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

x. FTP Integration
xi. HP iLO and OA
xii. HP Operations Manager
xiii. HP Service Manager
xiv. IBM Tivoli Netcool/OMNIbus
xv. Representational State Transfer (REST)
xvi. Sharepoint
xvii. VMware vSphere
xviii. System Center

3. Serwer zarządzający i baza danych:

a. Serwer zarządzający powinien organizować jednoczesny dostęp konsoli graficznych administratorów i zapewniać funkcje Check-In/Check-Out dla poszczególnych przebiegów uniemożliwiając jednoczesne zmiany tego samego przebiegu przez dwóch użytkowników.

b. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).

c. Baza danych systemu powinna przechowywać:

i. Definicje przebiegów procesów
ii. Stan uruchomionych przebiegów
iii. Informacje statusowe (logs)

iv. Dane konfiguracyjne systemu

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

1. Architektura:
    a. System musi posiadać serwer zarządzający odpowiedzialny za wykonywanie wszystkich zadań związanych z obsługą incydentów, problemów, zmian, zleceń, użytkowników, itp... zapewniając jednocześnie wymuszenie odpowiednich uprawnień.
    b. System musi posiadać zintegrowany komponent CMDB (Configuration Management Database)
    c. System musi posiadać zintegrowany moduł bazy wiedzy (Knowledge Management)
    d. System musi posiadać graficzną konsolę użytkownika instalowana lokalnie na komputerach pracowników wsparcia.
    e. System musi posiadać komponent hurtowni danych, odpowiedzialny za agregację i przechowywanie danych historycznych i przygotowywanie raportów.
    f. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
    g. System musi posiadać konsolę webową umożliwiającą pracownikom zgłaszanie incydentów/problemów technicznych oraz zapotrzebowania na zasoby IT.
2. Procesy wsparcia:
    a. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy:
        i. Zarządzanie incydentami
        ii. Zarządzanie problemami
        iii. Zarządzanie zmianą
        iv. Zarządzanie
    b. W zakresie zarządzania incydentami i problemami system powinien posiadać:
        i. Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:
            - Narażony użytkownik,
            - Alternatywna metoda kontaktu,
            - Tytuł,
            - Opis,
            - Kategoria,
            - Pilność,
            - Wpływ,

- Źródło,
- Grupa pomocy technicznej,
- Przypisany,
- Podstawowy właściciel,
- Uwzględnione usługi,
- Narażone elementy,
- Dziennik akcji (komentarz).

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

b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:

i. Konektor do systemu zarządzania infrastrukturą i oprogramowaniem

ii. Konektor do systemu zarządzania komponentami

iii. Konektor do systemu zarządzania środowiskami wirtualnym

iv. Konektor do systemu automatyzacji zarządzania środowisk IT

v. Konektor do usługi katalogowej

1. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
2. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
3. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
4. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:

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

Ochrona antymalware
Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem
3. Centralne zarządzanie politykami ochrony.

4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.).
10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

Oprogramowanie do zarządzania środowiskami serwerowymi typ I (licencja na 16 rdzeni procesora)
Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego rdzenia procesora fizycznego na serwerze. Liczba procesorów i ilość pamięci operacyjnej nie mogą mieć wpływu na liczbę wymaganych licencji. Każda licencja na 16 fizycznych rdzeni procesorów serwera musi uprawniać do zarządzania 2 (dwoma) środowiskami systemu operacyjnego na tym serwerze.
Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

- System zarządzania infrastrukturą i oprogramowaniem
- System zarządzania komponentami
- System zarządzania środowiskami wirtualnym

- System tworzenia kopii zapasowych
- System automatyzacji zarządzania środowisk IT
- System zarządzania incydentami i problemami
- Ochrona antymalware

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

7. Inwentaryzacja i zarządzanie zasobami:

    f. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania

    g. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu zarządzającego, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu

    h. 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...)

    i. 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

    j. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera

8. Użytkowane oprogramowanie – pomiar wykorzystania

    c. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania

    d. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.

9. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

    j. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika

    k. 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)

    l. 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

m. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek

n. 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

o. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil)

p. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie

q. 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)

r. System powinien być zintegrowany z oprogramowaniem antywirusowym i być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.

10. Definiowanie i sprawdzanie standardu serwera:

e. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,

f. Reguły powinny sprawdzać następujące elementy systemy komputerowego:

g. stan usługi

h. obecność poprawek (Hotfix)

i. narzędzie do zarządzania i dostępu do komponentów sprzętowo-programowych serwera

j. rejestr systemowy

k. system plików

l. usługę katalogową

m. SQL (query)

n. wewnętrzna baza danych serwera usług internetowych

o. 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.

11. Raportowanie, prezentacja danych:

g. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub

h. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services

i. System powinien posiadać predefiniowane raport w następujących kategoriach:

- Sprzęt (inwentaryzacja)
- Oprogramowanie (inwentaryzacja)
- Oprogramowanie (wykorzystanie)
- Oprogramowanie (aktualizacje, w tym system operacyjny)

j. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport

k. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu

l. 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.

12. Analiza działania systemu, logi, komponenty

c. 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

d. 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:

8. Architektura

d. System zarządzania komponentami powinien składać się z:
   - Serwera Zarządzającego,

- Serwer zarządzania jest punktem centralnym do zarządzanie grupą (pulą) serwerów i komunikowania się z bazą danych. Po otwarciu konsoli serwera możliwe jest podłączenie się do grupy zarządzającej, W zależności od wielkości środowiska komputerowego, grupa zarządzania może zawierać jeden lub wiele serwerów połączonych w pule zasobów.

- Bazy Operacyjnej przechowującej informacje o zarządzanych elementach,

  - baza operacyjna jest relacyjną bazą danych, która zawiera wszystkie dane konfiguracyjne dla zarządzanej grupy serwerów i przechowuje wszystkie dane związane z monitorowaniem. Baza Operacyjna zachowuje dane krótkoterminowe, domyślnie 7 dni.

- Baza Hurtowej przechowującej dane do analiz historycznych, definiuje granicę czasową do retencji danych historycznych.

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

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

j. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.

k. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.

l. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.

m. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.

n. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.

o. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.

p. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).

q. Wsparcie dla protokołu IPv6.

r. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.

9. Audyt zdarzeń bezpieczeństwa

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

d. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).

e. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.

f. 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.

10. Konfiguracja i monitorowanie

System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

h. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:

- rejestru
- narzędzie do zarządzania i dostępu do komponentów sprzętowo-programowych serwera
- OLEDB
- LDAP
- skrypty (uruchamiane w celu wykrycia atrybutów obiektu),

W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.

i. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp...

j. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:

- Windows Server 2003 SP2
- Windows 2008 Server SP2
- Windows 2008 Server R2
- Windows 2008 Server R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Client OS:
    - Windows XP Pro x64 SP2
    - Windows XP Pro SP32
    - Windows Vista SP2
    - Windows XP Embedded Standard

    - Windows XP Embedded Enterprise
    - Windows XP Embedded POSReady
    - Windows 7 Professional for Embedded Systems
    - Windows 7 Ultimate for Embedded Systems
    - Windows 7
    - Windows 8
    - Windows 8.1
- Active Directory 2003/2008
- Exchange 2003/2007/2010
- Microsoft SharePoint 2003/2007/2010
- Microsoft SharePoint Services 3.0
- Microsoft SharePoint Foundation 2010
- SQL 2005/2008/2008R2 (x86/x64/ia64)
- Information Worker (Office, IExplorer, Outlook, itp…)
- IIS 6.0/7.0/7.5
- Linux/Unix
    - HP-UX 11i V2 (PA-RISC and Itanium)
    - HP-UX 11i V3 (PA-RISC and Itanium)
    - Oracle Solaris 9 (SPARC)
    - Oracle Solaris 10 (SPARC and x86)
    - Oracle Solaris 11 (SPARC and x86)
    - Red Hat Enterprises Linux 4 (x86/x64)
    - Red Hat Enterprises Linux 5 (x86/x64)
    - Red Hat Enterprises Linux 6 (x86/x64)
    - SUSE Linux Enterprise Server 9 (x86)
    - SUSE Linux Enterprise Server 10 (x86/x64)
    - SUSE Linux Enterprise Server 11 (x86/x64)
    - IBM AIX 5.3 (POWER)
    - IBM AIX 6.1 (POWER)
    - IBM AIX 7.1 (POWER)
    - Cent OS 5 (x86/x64)
    - Cent OS 6 (x86/x64)

- Debian 5 (x86/x64)
- Debian 6 (x86/x64)
- Ubuntu Server 10.04 (x86/x64)
- Ubuntu Server 12.04 (x86/x64)

k. Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.

l. 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)

m. 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

n. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów

11. Tworzenie reguł

k. W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:

- Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event)
- Performance based (SNMP performance, WMI performance, Windows performance)
- Probe based (scripts: event, performance)

l. 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.

m. 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.

n. 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.

o. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.

p. 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

q. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.

r. 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).

s. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.

t. 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).

12. Przechowywanie i dostęp do informacji

    g. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp...) powinny być przechowywane w bazie danych operacyjnych.

    h. 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.

    i. 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).

    j. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.

    k. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.

    l. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:

        - XML
        - CSV
        - TIFF
        - PDF
        - XLS
        - Web archive

13. Konsola systemu zarządzania

    i. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.

    j. 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).

    k. 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).

l. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.

m. 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".

n. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.

o. 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

p. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).

14. 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:

5. Architektura

   d. 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.

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

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

6. Interfejs użytkownika

   f. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.

   g. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.

   h. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...

   i. 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.

   j. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.

7. Scenariusze i zadania

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

      3. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,

      4. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:

         iv. profilu sprzętowego

         v. profilu systemu operacyjnego,

         vi. przygotowanych dysków twardych,

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

k. 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

l. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.

m. 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.

n. 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.

o. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.

p. 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.

8. Wymagania dodatkowe

h. 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.

i. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.

j. 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

k. System musi umożliwiać skorzystanie z szablonów:

- wirtualnych maszyn
- usług

oraz profili dla:
- aplikacji
- serwera SQL

- hosta
- sprzętu
- systemu operacyjnego gościa

l. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).

m. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.

n. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją)

System tworzenia kopii zapasowych
System tworzenia i odtwarzania kopii zapasowych danych (backup) musi spełniać następujące wymagania:

6. 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)
7. Wykonywanie kopii zapasowych:
    a. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
    b. System kopii zapasowych musi posiadać możliwości zapisu danych na:
        i. na puli magazynowej złożonej z dysków twardych
        ii. na napędach I bibliotekach taśmowych
        iii. podłączonych zdalnie zasobach chmurowych
    c. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych
    d. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych
    e. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
    f. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych

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

g. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.

h. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.

i. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony:

   i. Krótkoterminowe: Pule dyskowe – do 448 dni

   ii. Online: Zasoby chmurowe – do 3360 dni

   iii. Krótkoterminowe: Taśmy – do 12 tygodni

   iv. Długoterminowe: Taśmy – do 99 lat

8. Odzyskiwanie danych:

   a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje"

   b. System kopii zapasowych musi umożliwiać odtworzenie danych do:

      i. lokalizacji oryginalnej

      ii. lokalizacji alternatywnej

      iii. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych

9. Agent kopii zapasowej

   a. Agent powinien posiadać możliwość współpracy z komponentami VSC.

   b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych" oraz wykorzystywanego pasma w i poza godzinami „biznesowymi"

   c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:

      i. System operacyjny Windows (w tym pliki, system state i BMR)

      ii. Maszyny wirtualne na platformie Hyper-V

      iii. Bazy danych MS SQL

      iv. Sharepoint

      v. Exchange

10. 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.

4. Architektura:

g. 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.

h. 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.

i. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.

j. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).

k. 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.

l. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).

5. Tworzenie przebiegów:

e. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.

f. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.

g. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:

i. System:

1. Run Program
2. Run .Net Script
3. End Process
4. Start/Stop Service
5. Restart System
6. Save Event Log
7. implementacji CIM Query
8. Run SSH Command
9. Get SNMP Variable
10. Monitor SNMP Trap
11. Send SNMP Trap
12. Set SNMP Variable

ii. Planowanie:

1. Monitor Date/Time
2. Check Schedule

iii. Monitorowanie:

1. Monitor Event Log
2. Monitor Service
3. Get Service Status
4. Monitor Process
5. Get Process Status
6. Monitor Computer/IP Status
7. Monitor Disk Space
8. Get Disk Space Status
9. Monitor Internet Application
10. Get Internet Application Status
11. pozostałych komponentów sprzętowych serwera

iv. Zarządzanie plikami:

1. Compress File
2. Copy File
3. Create Folder
4. Decompress File

5. Delete File
6. Delete Folder
7. Get File Status
8. Monitor File
9. Monitor Folder
10. Move File
11. Move Folder
12. PGP Decrypt File
13. PGP Encrypt File
14. Print File
15. Rename File

v. E-mail:

1. Send E-mail

vi. Powiadomienia:

1. Send Event Log Message
2. Send Syslog Message
3. Send Platform Event

vii. Narzędzia:

1. Apply XSLT
2. Query XML
3. Map Published Data
4. Compare Values
5. Write Web Page
6. Read Text Log
7. Write to Database
8. Query Database
9. Monitor Counter
10. Get Counter Value
11. Modify Counter
12. Invoke Web Services
13. Format Date/Time
14. Generate Random Text

15. Map Network Path
16. Disconnect Network Path
17. Get Dial-up Status
18. Connect/Disconnect Dial-up

viii. Zarządzanie plikami tekstowymi:

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

ix. Kontrola przepływów (runbooks):

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

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

x. FTP Integration
xi. HP iLO and OA
xii. HP Operations Manager
xiii. HP Service Manager
xiv. IBM Tivoli Netcool/OMNIbus
xv. Representational State Transfer (REST)
xvi. Sharepoint
xvii. VMware vSphere
xviii. System Center

6. Serwer zarządzający i baza danych:

d. 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.

e. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).

f. Baza danych systemu powinna przechowywać:

   i. Definicje przebiegów procesów

   ii. Stan uruchomionych przebiegów

   iii. Informacje statusowe (logs)

   iv. Dane konfiguracyjne systemu

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

4. 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.

5. Procesy wsparcia:

   a. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy:

      i. Zarządzanie incydentami

      ii. Zarządzanie problemami

      iii. Zarządzanie zmianą

      iv. Zarządzanie

   b. W zakresie zarządzania incydentami i problemami system powinien posiadać:

      i. Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:

         - Narażony użytkownik,

         - Alternatywna metoda kontaktu,

- Tytuł,
- Opis,
- Kategoria,
- Pilność,
- Wpływ,
- Źródło,
- Grupa pomocy technicznej,
- Przypisany,
- Podstawowy właściciel,
- Uwzględnione usługi,
- Narażone elementy,
- Dziennik akcji (komentarz).

6. Komponent CMDB:
    a. Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym:
        i. Użytkownik:
            - Imię
            - Nazwisko
            - Inicjały
            - Tytuł,
            - Firma,
            - Dział,
            - Biuro,
            - Telefon służbowy,
            - Ulica i numer,
            - Miejscowość,
            - Województwo,
            - Kod pocztowy,
            - Kraj,
            - Strefa czasowa,
            - Ustawienia regionalne,

- Komputery użytkownika
- Urządzenia użytkownika
- Elementy pokrewne (incydenty, problemy, zmiany, itp...)

ii. Komputer:

b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:

i. Konektor do systemu zarządzania infrastrukturą i oprogramowaniem

ii. Konektor do systemu zarządzania komponentami

iii. Konektor do systemu zarządzania środowiskami wirtualnym

iv. Konektor do systemu automatyzacji zarządzania środowisk IT

v. Konektor do usługi katalogowej

5. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
6. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
7. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
8. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:

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

Ochrona antymalware
Oprogramowanie antymalware musi spełniać następujące wymagania:

12. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
13. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem
14. Centralne zarządzanie politykami ochrony.
15. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
16. Mechanizmy wspomagające masową instalację.
17. 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.
18. 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.
19. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
20. 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.).
21. 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.
22. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.

Serwerowy system operacyjny (licencja na 16 rdzeni procesora)

Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi

pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.
Serwerowy system operacyjny 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) 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:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.

d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

   i. Dystrybucję certyfikatów poprzez http

   ii. Konsolidację CA dla wielu lasów domeny,

   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. Szyfrowanie plików i folderów.

g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h. 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 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:

   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

   iii. Obsługi 4-KB sektorów dysków

   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

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.

Serwerowy system operacyjny (licencja na 16 rdzeni procesora)

Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

32. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
33. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
34. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
35. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
36. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
37. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
38. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
39. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
40. 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).

41. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
42. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
43. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
44. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
45. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
46. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
47. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
48. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
49. 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),
50. 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..
51. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
52. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
53. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
54. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
55. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
56. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    n. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

o. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

   i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

   ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

   iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

   iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

p. Zdalna dystrybucja oprogramowania na stacje robocze.

q. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

r. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

   i. Dystrybucję certyfikatów poprzez http

   ii. Konsolidację CA dla wielu lasów domeny,

   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

s. Szyfrowanie plików i folderów.

t. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

u. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

v. Serwis udostępniania stron WWW.

w. Wsparcie dla protokołu IP w wersji 6 (IPv6),

x. Wsparcie dla algorytmów Suite B (RFC 4869),

y. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

z. Wbudowane mechanizmy wirtualizacji 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:

   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

57. 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.
58. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
59. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
60. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
61. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Serwer relacyjnej bazy danych typ II

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

1. Możliwość wykorzystania SBD, jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Wykonywanie typowych zadań administracyjnych w trybie on-line - SBD musi umożliwiać wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie

danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednoużytkownikowy.

6. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
7. Skalowalność systemu - SBD powinien wspierać skalowanie w kontekście wielkości rozwiązania (powinien być dostępny zarówno na platformie wieloserwerowej, jak również średniej wielkości komputerów i urządzeń mobilnych).
8. Możliwość dodawania procesorów bez restartu systemu - SBD powinien umożliwiać dodanie procesora do systemu, bez konieczności restartu silnika bazy danych.
9. Kopie bazy tylko do odczytu - SBD powinien umożliwiać tworzenie w dowolnym momencie kopii bazy danych tylko do odczytu zawierającej stan bazy z bieżącego momentu czasu. Wiele takich kopii może być równolegle użytkowanych w celu wykonywania z nich zapytań.
10. Możliwość dodawania pamięci bez restartu systemu - SBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych.
11. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych.
12. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między wieloma lokalizacjami (podstawowa i zapasowe) przy zachowaniu następujących cech:
    - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
    - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
    - duplikacja danych w trybie synchronicznym lub asynchronicznym,
    - SBD musi umożliwiać duplikację danych z ośrodka podstawowego, do co najmniej 8 lokalizacji zapasowych,
    - w celu zwiększenia skalowalności i wydajności systemu SBD musi umożliwiać korzystanie z kopii baz w lokalizacjach zapasowych w trybie tylko do odczytu (raportowanie, tworzenie backupów itp.) bez przerywania działania mechanizmu duplikacji danych z ośrodka podstawowego,
    - klienci bazy danych mogą być automatycznie przełączeni do bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
    - brak limitu odległości miedzy systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza oraz limity wynikające z opóźnień na łączu),
    - kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenie sieci),
    - system automatycznie naprawia błędy pamięci masowej (w przypadku odkrycia błędu fizycznego odczytu danych z pamięci masowej, poprawny fragment danych jest transferowany z drugiego systemu i korygowany).
13. Replikacja danych i modyfikacja w wielu punktach - SBD powinien pozwalać na transakcyjną replikację wybranych danych z bazy danych między wieloma węzłami. Dodanie lub usunięcie węzła nie powinno wpływać na funkcjonowanie i spójność systemu replikacji, ani nie powinno przerywać procesu replikacji. Dane mogą w takim schemacie replikacji być modyfikowane w dowolnym węźle, (ale tylko w jednym węźle w danym momencie). System

powinien zawierać narzędzie do nadzorowania i wizualizacji topologii oraz stanu procesu replikacji. Dodatkowo SBD powinien umożliwiać kompresję przesyłanych danych między serwerami uczestniczącymi w replikacji, aby minimalizować obciążenie łączy sieciowych.

14. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
15. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania powinien wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
16. Możliwość szyfrowania przechowywanych danych - SBD musi pozwalać na szyfrowanie przechowywanych danych. Szyfrowanie musi być cechą SBD i nie może wymagać jakichkolwiek zmian w aplikacjach korzystających z danych. Zaszyfrowanie lub odszyfrowanie danych nie powinno powodować przerwy w dostępie do danych. Kopia bezpieczeństwa szyfrowanej bazy także powinna być automatycznie zaszyfrowana.
17. Korzystanie z zewnętrznych urządzeń do przechowywania kluczy szyfrujących - SBD powinien posiadać mechanizm pozwalający na przechowywanie kluczy szyfrujących na urządzeniach zewnętrznych (np. czytniki kart). Rozwiązanie to powinno być otwarte, to znaczy pozwalać na dodawanie w przyszłości obsługi urządzeń nowych, oczywiście pod warunkiem dostarczenia przez producenta urządzenia odpowiednich modułów oprogramowania zgodnych z SBD.
18. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w organizacji - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową.
19. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
20. Ograniczenie użycia zasobów – SBD powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, % wykorzystania pamięci, liczba operacji wejścia/wyjścia podsystemu dyskowego). Reguły definiujące ograniczenia dla użytkowników lub grup użytkowników dotyczące wykorzystania zasobów powinny mieć możliwość użycia w nich logiki zaimplementowanej za pomocą języka programowania (np. używanego w danym SBD języka SQL).
21. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
22. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie

asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.

23. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych powinien udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).
24. System SDB musi łączyć w sobie cechy bazy przechowywanej w pamięci RAM (IMDB) oraz tradycyjnej bazy danych (RDBMS) przechowywanej na dyskach.
25. System SDB musi zapewniać w ramach tej samej bazy danych możliwość umieszczenia wybranych tabel w pamięci RAM serwera, a pozostałych tabel w tradycyjnej postaci (na dysku).
26. SBD musi posiadać możliwość korzystania w procedurach jednocześnie z tabel przechowywanych w pamięci RAM oraz tabel przechowywanych na dyskach.
27. System SDB musi zapewniać wersjonowanie wierszy w tabelach przechowywanych w pamięci RAM.
28. W celu zwiększenia wydajności SBD musi posiadać możliwość tworzenia procedur składowanych w kodzie natywnym, to znaczy takich procedur, które są automatycznie kompilowane do kodu natywnego podczas ich tworzenia oraz składają się z instrukcji procesora, które nie wymagają dalszych kompilacji lub interpretacji.
29. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń (rejestrowanie tylko zdarzeń spełniających zdefiniowane warunki filtrujące, np. dotyczących tylko wskazanego obiektu). Wymagana jest rejestracja zdarzeń:
    - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
    - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
    - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).
30. Możliwość rejestrowania bardzo dużej liczby zdarzeń i analizowania ich z minimalnym opóźnieniem – SBD powinien dostarczać wbudowaną platformę do tworzenia aplikacji typu CEP (Complex Event Processing). Aplikacje takie umożliwiają rejestrowanie bardzo dużej liczby zdarzeń (np. odczytów liczników lub z innych urządzeń pomiarowych, dowolnych zdarzeń występujących z dużą częstotliwością) i reagowanie na nie z minimalnym opóźnieniem. System powinien również udostępniać mechanizmy wysokiej dostępności dla tej usługi.
31. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
32. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku

programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.

33. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
    - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
    - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
    - udostępniać język zapytań do struktur XML,
    - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
    - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.
34. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
    - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
    - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
    - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
    - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).
35. Możliwość efektywnego przechowywania dużych obiektów binarnych - SBD powinien umożliwiać przechowywanie i efektywne zarządzanie dużymi obiektami binarnymi (pliki graficzne, multimedialne, dokumenty, itp.). Obiekty te nie powinny być przechowywane w plikach bazy danych, ale w systemie plików. Jednocześnie pliki te powinny być zarządzane przez SBD (kontrola dostępu na podstawie uprawnień nadanych w SBD). Dodatkowo dane binarne powinny być dostępne dla użytkowników bazy danych jako standardowa kolumna tabeli (dostęp z poziomu zapytań języka SQL obsługiwanego przez SBD).
36. Możliwość kompresji przechowywanych danych - SBD powinien udostępniać wbudowany mechanizm kompresji zgromadzonych danych w celu osiągnięcia lepszej wydajności przy niezmienionej konfiguracji sprzętowej. System kompresji powinien umożliwiać również kompresję UNICODE systemem UCS-2.
37. Możliwość rejestracji zmiany w rekordzie danych – SBD powinien pozwalać na rejestrację zmian w danych włącznie z zapamiętaniem stanu pojedynczego rekordu danych sprzed modyfikacji. Rozwiązanie nie powinno ujemnie wpływać na wydajność systemu i powinno być konfigurowalne bez wpływu na istniejące aplikacje korzystające z danych. Rozwiązanie powinno rejestrować także zmiany w definicji struktur danych.

38. Audyt dostępu do danych - SBD powinien pozwalać na rejestrację operacji takich jak: logowanie, wylogowanie użytkownika, zmiany w definicji obiektów bazy danych (tabele, procedury), wykonywanie przez wskazanego użytkownika operacji takich jak SELECT, INSERT, UPDATE, DELETE. Rozwiązanie powinno być niezależne od aplikacji, wbudowane w SBD.
39. Partycjonowanie danych - SBD powinien pozwalać na podział danych w jednej tabeli między różne fizyczne pamięci masowe zgodnie ze zdefiniowanymi warunkami podziału. Powinien udostępniać mechanizm równoległego (wielowątkowego) dostępu do danych umieszczonych w różnych partycjach. Dodatkowo powinna być dostępna możliwość szybkiego przesyłania dużych zbiorów danych poprzez mechanizm przełączania partycji (czyli dane przenoszone są z jednej tabeli do drugiej za pomocą operacji na metadanych, a nie przez fizyczne kopiowanie rekordów). Dzięki takiej funkcjonalności możliwe jest przeniesienie dużej liczby rekordów w bardzo krótkim czasie (rzędu sekund). Dodatkowo minimalizowane jest odczuwanie wpływu tej operacji przez użytkowników (minimalny wpływ przenoszenia danych na obciążenie systemu).
40. Wsparcie dla Indeksów kolumnowych - SBD powinien umożliwiać tworzenie indeksów przechowujących dane osobno dla każdej z kolumn tabeli łącząc je następnie w całość. Indeks powinien również wykorzystywać mechanizm kompresji oraz pozwalać na modyfikowanie danych w tabeli, dla której taki indeks utworzono.
41. Indeksowanie podzbioru danych w tabeli - SBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące.
42. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System powinien umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo powinien udostępniać środowisko do debuggowania.
43. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
44. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
45. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
46. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.
47. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów

poddawanych transformacjom. Zestaw standardowych dostępnych transformacji powinien obejmować takie transformacje jak: sortowanie, wyszukiwanie wartości według klucza w tabelach słownikowych, automatyczna obsługa SCD (*Slowly Changing Dimension*) w zasilaniu hurtowni danych, pobranie danych z serwera FTP, wysłanie e-maila, łączenie danych z wykorzystaniem logiki rozmytej, poprawa jakości danych wykorzystująca integrację z dedykowanym systemem zarządzania jakością danych oraz jego bazą wiedzy i reguł walidujących. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:

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

48. SBD musi umożliwiać odpytywanie danych w klastrach Hadoop za pomocą języka SQL. System musi umożliwiać łączenie w ramach jednego zapytania SQL danych pozostających w relacyjnej bazie danych oraz danych składowanych w klastrze Hadoop. Dodatkowo system musi, tam gdzie jest to uzasadnione wydajnościowo, wykorzystywać możliwości przetwarzania klastra Hadoop generując adekwatne zadania MapReduce.
49. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (hurtownia danych). System powinien umożliwiać pracę w dwóch trybach: wielowymiarowym (tworzenie kostek wielowymiarowych), tabelarycznym (wykorzystującym technologię in-memory BI). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
50. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie

zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. System powinien pozwalać na integrację z relacyjną bazą danych –wymagana jest możliwość uruchomienia procesu wyliczenia agregacji zainicjowana poprzez dodanie rekordu do tabeli w relacyjnej bazy danych. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).

51. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
52. Narzędzia do zarządzania jakością danych - SBD powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:
    - udostępniać funkcje do profilowania danych (analiza i raporty dotyczące jakości danych),
    - udostępniać funkcje do deduplikacji danych,
    - określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną do akceptacji przez użytkownika,
    - umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów),
    - umożliwiać definiowanie złożonych domen (zestawu kilku atrybutów) oraz ocenę jakości danych na podstawie powiązań między tymi atrybutami (np. weryfikację poprawności danych adresowych złożonych z kodu pocztowego, miasta i ulicy),
    - pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania),
    - umożliwiać eksport wyników badania (poprawnych i sugerowanych wartości) do pliku tekstowego lub bazy relacyjnej, eksport powinien obejmować wartości po korekcie oraz ewentualnie te przed korektą,
    - przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy),
    - umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych,
    - zapewniać mechanizmy „uczenia się" bazy wiedzy, czyli w miarę realizacji kolejnych procesów ręcznego czyszczenia danych baza wiedzy powinna umożliwiać gromadzenie tych informacji na potrzeby kolejnych procesów,
    - umożliwiać wykorzystanie bazy wiedzy w automatycznym procesie czyszczenia danych (powinien integrować się z narzędziami do ekstrakcji, transformacji i ładowania danych, dzięki czemu będzie można wykorzystać te mechanizmy w automatycznym procesie ładowania danych).
53. Możliwość zarządzania centralnymi słownikami danych - SBD powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM).

    System MDM powinien:
    - udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach,

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

54. Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
55. Wbudowany system analityczny musi umożliwiać rejestrowanie zapytań wykonywanych przez użytkowników, a następnie umożliwiać na podstawie zgromadzonych informacji na automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).
56. Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
57. Wbudowany system analityczny powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych.
58. Wbudowany system analityczny powinien umożliwiać tworzenie perspektyw na bazie wielowymiarowej pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych w całej bazie danych.
59. Wbudowany system analityczny powinien umożliwiać użytkownikom tworzenie analiz In-Memory, czyli przetwarzanie dużej liczby rekordów skompresowanych w pamięci RAM. Powinien umożliwiać tworzenie modeli wykorzystujących tabele pochodzące z wielu niezależnych źródeł danych i łączone między sobą relacjami.
60. Wbudowany system analityczny powinien udostępniać dedykowany język do tworzenia logiki biznesowej w modelu. Język ten powinien m.in. obsługiwać relacje utworzone między tabelami, mechanizmy time intelligence (operacje na datach i okresach) oraz zapewniać mechanizmy kontroli bezpieczeństwa i dostępu do danych na poziomie poszczególnych wierszy.
61. Wbudowany system analityczny powinien dostarczać kreatory modelowania złożonych procesów biznesowych, pozwalających w prosty sposób niezaawansowanym użytkownikom implementować złożone problemy analizy biznesowej w modelu analitycznym, czyniąc programowanie projektów BI przystępnym dla większej liczby osób i organizacji.
62. Wsparcie dla optymalizacji zapytań z modelu gwiazdy (fakty-wymiary) - SBD powinien udostępniać mechanizmy optymalizacji zapytań w modelu gwiazdy (tabela faktów łączona z tabelami wymiarów). Zapytania te często wykorzystywane są w hurtowniach danych i analizach wielowymiarowych. Ze względu na dużą liczbę danych wykorzystywanych w tego typu zapytaniach metody optymalizacji tego typu zapytań pozwalają znacząco zwiększyć wydajność przy tworzeniu rozwiązań hurtowni danych i wielowymiarowych struktur analitycznych (OLAP).

63. Wsparcie dla zapytań aktualizujących tabele faktów w modelach wielowymiarowych - SBD powinien udostępniać wbudowane mechanizmy pozwalające w łatwy i szybki sposób aktualizować zawartość tabel faktów (wykorzystywanych w modelach wielowymiarowych). Mechanizm ten powinien być dostępny z poziomu zapytań języka SQL obsługiwanego przez silnik bazy danych.
64. Aktywne buforowanie danych Proactive caching - SBD powinien udostępniać mechanizm odświeżania danych w strukturach wielowymiarowych, który wykrywa zmiany w systemach źródłowych i na bieżąco aktualizuje bazę wielowymiarową.
65. Wbudowany system analityczny powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane).
66. Wbudowany system analityczny powinien mieć wbudowaną funkcję importu tabelarycznych modeli danych wykorzystujących technologię in-memory BI i przygotowanych w aplikacji Microsoft Excel. Podczas procesu importu na serwerze model powinien być odtwarzany w postaci bazy danych.
67. Wbudowany system analityczny powinien umożliwiać zasilanie modelu tabelarycznego m.in. z następujących systemów źródłowych: bazy relacyjne, bazy wielowymiarowe, modele tabelaryczne, zbiory danych przechowywane w usługach chmury publicznej, pliki płaskie, inne raporty udostępniane w formacie Atom 1.0.
68. Wbudowany system analityczny powinien umożliwiać działanie modelu tabelarycznego w dwóch trybach – z użyciem buforowania (możliwe opóźnienie, ale większa wydajność) oraz bez użycia buforowania (zapytania użytkowników końcowych korzystających z modelu są przesyłane bezpośrednio do źródłowej bazy relacyjnej i zwracają najbardziej aktualną wersję danych).
69. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system powinien udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
70. System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining
71. Wbudowany system analityczny musi posiadać natywne wsparcie dla obsługi zaawansowanych analiz w języku R. Musi istnieć możliwość wywołania skryptu R w ramach zapytania SQL oraz osadzania takiego skryptu jako procedury składowanej.
72. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. System powinien umożliwiać tworzenie takich wskaźników również w modelach danych wykorzystujących technologię in-memory BI.
73. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Raporty powinny być udostępnianie przez system protokołem HTTP, bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:
    - raporty parametryzowane,

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

74. Raporty udostępniane przez SBD muszą być poprawnie wyświetlane w przeglądarkach zgodnych z HTML 5, bez użycia dodatkowych wtyczek i rozszerzeń takich jak m.in.: Adobe Flash Player, Microsoft Silverlight, etc.
75. System raportowy SBD musi wspierać wyświetlanie raportów na urządzeniach mobilnych – system musi udostępniać bez dodatkowych kosztów natywne aplikacje min. dla systemów iOS, Android, Windows Phone.
76. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
77. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
78. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
79. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL).
80. Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
81. Narzędzia do tworzenia raportów ad-hoc - SBD powinien udostępniać narzędzia do tworzenia raportów ad-hoc przez niezaawansowanych użytkowników. Tworzenie raportów powinno odbywać się w środowisku graficznym. Użytkownicy powinni mieć możliwość na publikowanie stworzonych raportów na serwerze w celu udostępnienia ich szerszemu gronu osób.

Załącznik nr 2
do Umowy nr ...../14/BŁiI/17/DG/PMP

Wymagania gwarancyjne i serwisowe

1. Okres gwarancji na przedmiot umowy wynosi ..... miesięcy, przy czym bieg okresu gwarancyjnego rozpocznie się z chwilą podpisania bez zastrzeżeń końcowego protokołu odbioru Produktu.
2. Zamawiający zastrzega sobie prawo do dokonywania wszelkich zmian w przygotowanej na potrzeby odbioru ilościowo-jakościowego konfiguracji dostarczonego sprzętu bez naruszenia warunków gwarancyjnych i serwisowych.
3. Wykonawca dostarczy Zamawiającemu do akceptacji wzór karty gwarancyjnej dla Przedmiotu umowy.
4. Wszystkie urządzenia dostarczone przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów na rynek Polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem Wykonawcy, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu w języku polskim, najpóźniej w dniu dostawy oferowanych urządzeń do odbioru jakościowego.
5. Do dostarczonego sprzętu będą dołączone karty gwarancyjne zawierające numery seryjne produktu, numery seryjne oprogramowania, termin i warunki ważności gwarancji (zgodnie z umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
6. W ramach realizacji Przedmiotu umowy Wykonawca zapewni świadczenie usług gwarancyjnych..
7. Wsparcie producenta oprogramowania ma zapewniać dostarczanie łat bezpieczeństwa, poprawki i zmiany dotyczące działania samego produktu. Zapewni również też możliwość zgłaszania konieczności przygotowania poprawki czy też chęci zmiany w produkcie, konsultacji w zakresie aspektów technicznych czy licencyjnych i dostęp do bazy wiedzy.
8. Przez **usunięcie awarii krytycznej lub zwykłej** należy rozumieć przywrócenie pierwotnej funkcjonalności. Wykonawca zobowiązuje się do reinstalacji, konfiguracji/rekonfiguracji systemu/bazy danych dostarczonego w ramach Umowy po usunięciu awarii krytycznej lub zwykłej, jeżeli zachodzi taka konieczność.
9. Jeżeli w trakcie trwania gwarancji którykolwiek z elementów sprzętowych rutynowo podlegający okresowej wymianie, będzie sygnalizował konieczność wymiany (koniec okresu eksploatacji), zostanie wymieniony na fabrycznie nowy pozbawiony wad, (zgodnie z rekomendacją producenta) na koszt Wykonawcy w ramach Umowy. Dotyczy to w szczególności wszelkich baterii i/lub akumulatorów wchodzących w skład Przedmiotu umowy także w przypadku wykrycia usterek stwarzających możliwość (wzrost prawdopodobieństwa) wystąpienia awarii w przyszłości.
10. Wykonawca zobowiązuje się do dokonywania napraw w miejscu instalacji.
11. Wykonawca ma obowiązek przeprowadzić analizę wpływu zaproponowanych zmian wynikających z naprawy każdej awarii i przedstawi ją Zamawiającemu przed ich ewentualną implementacją do akceptacji wraz ze wskazaniem ewentualnych zagrożeń i skutków ubocznych zaproponowanych czynności. W przypadku braku akceptacji Wykonawca zobowiązany jest do przedstawienia rozwiązania alternatywnego.
12. Wykonawca ma obowiązek informowania Zamawiającego o wydaniu patchy i aktualizacji do oprogramowania wewnętrznego urządzeń (firmware), systemu operacyjnego, bazy danych i każdego innego oprogramowania objętego Umową. Informację w formie raportu Wykonawca będzie dostarczał Zamawiającemu w trakcie wykonywania przeglądów technicznych opisanych w pkt. 19, lub na żądanie Zamawiającego. Zamawiający zadecyduje, które z proponowanych aktualizacji oprogramowania zostaną przez Wykonawcę zainstalowane. Po uzyskaniu zgody Zamawiającego Wykonawca w terminie wyznaczonym przez Zamawiającego dokona aktualizacji w cenie Umowy bez naruszania praw autorskich producenta. Wykonawca do każdej aktualizacji będzie dołączał informacje, co zmienia dana aktualizacja i jakie są przesłanki do jej instalacji. Wykonawca sprawdzi poprawność działania sprzętu,systemu operacyjnego i bazy danych po zainstalowaniu aktualizacji. W przypadku wystąpienia nieprzewidzianych, niepożądanych

skutków wprowadzonych zmian Wykonawca zobowiązany jest do ich wycofania na żądanie Zamawiającego, przywracając poprawne działanie sprzętu, systemu operacyjnego i bazy danych do stanu przed aktualizacji

13. Uszkodzone elementy będą wymieniane w ramach Umowy przez Wykonawcę na nowe, sprawne, o parametrach nie gorszych od uszkodzonych, w ramach świadczenia napraw gwarancyjnych. Wymienione elementy będą odtąd stanowiły własność Zamawiającego. Elementy uszkodzone, poza dyskami twardymi i innymi nośnikami danych, będą zwracane Wykonawcy.
14. Dyski twarde będą wymieniane na nowe (z zastrzeżeniem punktu 15), pozbawione wad o parametrach nie gorszych, także w przypadku wykrycia usterek stwarzających możliwość (wzrost prawdopodobieństwa) wystąpienia awarii w przyszłości.
15. Jeżeli w trakcie trwania okresu gwarancyjnego którykolwiek z komponentów sprzętowych ulegnie awarii i nie będzie posiadał wsparcia producenta, zostanie wymieniony na koszt Wykonawcy na inny równoważny lub o lepszych parametrach technicznych, posiadający wsparcie producenta chyba, że Strony postanowią inaczej. Zamawiający będzie wymagał od Wykonawcy, potwierdzenia zawierającego informację z datami końca wsparcia producenta dla poszczególnych elementów sprzętu i oprogramowania systemowego w przypadku, gdy takie dane zostaną przez producenta opublikowane (oficjalnie przez producenta ogłoszone) lub, gdy Wykonawca posiada taką wiedzę z innego niż publikacja źródła.
16. Dwukrotne uszkodzenie tego samego komponentu sprzętowego zaistniałe w okresie gwarancji obliguje Wykonawcę do wymiany tego komponentu sprzętowego na nowy, wolny od wad, równoważny funkcjonalnie, z zastrzeżeniem punktu 15, w terminie 5 dni od daty ostatniego zgłoszenia. Okres gwarancji określony w pkt. 1 dla wymienionego sprzętu rozpocznie się z chwilą jego dostarczenia.
17. W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez Wykonawcę na nowy, wolny od wad, równoważny funkcjonalnie, bez konieczności zwrotu uszkodzonego dysku twardego lub innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
18. Fakt awarii, naprawy i ewentualnie wymiany sprzętu na nowy będzie każdorazowo odnotowany w karcie gwarancyjnej urządzenia chyba, że strony uzgodnią inna formę dokumentowania, uwzględniającą warunki gwarancyjne producenta.
19. W trakcie trwania gwarancji Wykonawca przeprowadzi udokumentowane przeglądy techniczne oraz konserwacje, w tym czyszczenie wszystkich komponentów sprzętowych dostarczonego sprzętu i dokona wynikających z zaleceń producenta czynności serwisowych zgodnie z opracowanym przez Wykonawcę i zatwierdzonym przez Zamawiającego Harmonogramem prac (który zostanie dostarczony Zamawiającemu z chwilą podpisania protokołu odbioru ilościowo-jakościowego). Każdy z komponentów, objęty gwarancją musi przejść przegląd i czynności wynikające z zaleceń minimum raz w roku. Czynności te muszą w szczególności zawierać: przeglądy techniczne w tym przeglądanie i analizę logów sprzętowych i systemowych oraz weryfikację poprawności konfiguracji infrastruktury sprzętowej i systemu operacyjnego z uwzględnieniem zapisów z pkt.11. W ramach przeglądów Wykonawca również zobowiązuje się przeprowadzić prewencyjne wymiany części, które wykazują usterki mogące skutkować awarią. Ww. czynności muszą być tak zaplanowane i przygotowane aby w przypadku fizycznego wyłączenia/restartu sprzętu, maksymalnie zminimalizować ewentualne przestoje systemu/sprzętu. Wszystkie wymienione czynności muszą być uzgodnione z Zamawiającym i udokumentowane.
20. Wykonawca w przypadku wyłączenia systemu i/lub wystąpienia awarii sprzętu, zobowiązany jest do współpracy z Wykonawcą świadczącym serwis aplikacji, w celu doprowadzenia funkcjonalności systemów do stanu sprzed wyłączenia systemu i/lub awarii.
21. Wykonawca zobowiązuje się do wykonywania prac konserwacyjnych zgodnie z zasadami prawidłowej eksploatacji sprzętu określonymi przez producenta.
22. Zgłoszenia wszystkich awarii będą przyjmowane przez Wykonawcę w trybie 24/7 w Systemie Obsługi Zgłoszeń lub pocztą elektroniczną email, faksem, telefonicznie lub w inny ustalony sposób. Wykonawca może odmówić przyjęcia zgłoszenia, jeżeli:

    a) zostało ono dokonane przez osobę nieuprawnioną;

    b) zgłoszenie dotyczy obszaru, który nie jest objęty zakresem Umowy.

W przypadku odmowy przyjęcia zgłoszenia Wykonawca poinformuje o tym fakcie Zamawiającego po otrzymaniu zgłoszenia podając w formie pisemnej (e-mail lub fax) przyczynę odmowy.

23. Wykonawca zobowiązuje się do usunięcia awarii krytycznej **w ciągu ..... godzin** od chwili jej zgłoszenia (**max. 24 godziny**).
24. Wykonawca zobowiązuje się do usunięcia awarii zwykłej **w ciągu 48 godzin** od chwili jej zgłoszenia.
25. Wykonawca zobowiązuje się do potwierdzenia w formie pisemnej (e-mail lub fax) przyjęcia zgłoszenia awarii krytycznej i zwykłej od uprawnionego przedstawiciela Zamawiającego w przeciągu 1 godziny od chwili otrzymania zgłoszenia.
26. Czas na usunięcie każdej awarii będzie liczony od momentu wysłania zgłoszenia awarii do momentu potwierdzenia jej usunięcia przez uprawnionych przedstawicieli Zamawiającego.
27. Wykonawca w **terminie 5 dni** od dnia zawarcia Umowy dostarczy Zamawiającemu (do akceptacji) procedury zgłaszania i obsługi awarii wraz z wykazem adresów poczty elektronicznej, nr telefonów, nr faksów, adresu Systemu Obsługi Zgłoszeń, itp.
28. Wykonawca zapewni obsługę zgłaszania każdej awarii i pomocy technicznej w języku polskim.
29. Wszystkie czynności serwisowe wymagające kontaktu z personelem Zamawiającego muszą być wykonywane przez osoby biegle mówiące w języku polskim.
30. Do zgłaszania awarii upoważnione są osoby wymienione na liście osób uprawnionych do dokonywania zgłoszeń, dostarczonej do Wykonawcy przez Zamawiającego w **terminie 5 dni** roboczych od dnia zawarcia umowy. W trakcie trwania gwarancji lista osób uprawnionych do dokonywania zgłoszeń do Wykonawcy może być modyfikowana przez Zamawiającego. Każda zmiana musi zostać przekazana przez Zamawiającego, na co najmniej 3 dni robocze przed jej wejściem w życie.
31. Wykonawca zobowiązuje się, że nie będzie dokonywał żadnych modyfikacji sprzętu bez wcześniejszego uzgodnienia z Zamawiającym. Zamawiający zastrzega sobie prawo do samodzielnej rozbudowy sprzętu i dokonywania zmian w konfiguracji. Zamawiający poinformuje Wykonawcę o samodzielnej rozbudowie i zmianach w konfiguracji.
32. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.
33. Dla oprogramowania obowiązują prawa gwarancyjne producenta.
34. W wypadku rozbieżności pomiędzy postanowieniami Umowy, a postanowieniami kart gwarancyjnych, pierwszeństwo mają postanowienia Umowy.
35. Świadczenie na rzecz Zamawiającego usług serwisu gwarancyjnego oraz korzystanie z uprawnień wynikających z gwarancji, w tym odbiór z siedziby Zamawiającego sprzętu do naprawy i jego zwrot po naprawie, bądź dostawa wymienionego sprzętu zawarte jest w wynagrodzeniu, o którym mowa w § 2 ust. 1 Umowy.
36. Logi systemowe, o których mowa w pkt. 19 nie zawierają informacji dotyczących dostępu do bazy danych w tym również w trybie bezpośrednim.
37. Wykonawca świadczący serwis gwarancyjny sprzętu, w przypadku wyłączenia systemu i/lub wystąpienia awarii sprzętu, zobowiązany jest do współpracy z Wykonawcą świadczącym serwis aplikacji lub Zamawiającym (podczas samodzielnych prac serwisowych aplikacji), w celu doprowadzenia funkcjonalności systemów do stanu sprzed wyłączenia systemu i/lub awarii.
38. W ramach wsparcia gwarancyjnego Wykonawca zapewni stały kontakt w Dni Robocze w godzinach 8.15-16.15, w celu udzielania Konsultacji technicznych w zakresie objętym Umową, w tym również definiowania wymagań dla konfiguracji sprzętu i systemu operacyjnego oraz pracy systemów operacyjnych zainstalowanych na serwisowanym sprzęcie.
39. Ustala się następujący czas na udzielenie Konsultacji:
    - 16 godzin roboczych od momentu zgłoszenia dla Konsultacji. Czas udzielenia Konsultacji liczony będzie w godz. 8.15-16.15. Zgłoszenia Konsultacji będą następowały w Dni Robocze w godzinach 8.15-16.15

Załącznik nr 3
do Umowy nr ...../14/BŁiI/17/DG/PMP

Wymagania w zakresie szkoleń

I – Wymagania ogólne.

1. W ramach Umowy Wykonawca przeprowadzi następujące szkolenia:
   1.1. Szkolenia kadry Policji w zakresie nowych wersji systemów operacyjnych i baz danych oraz obsługi mechanizmów do zarządzania i monitorowania SWOP.
   1.2. Szkolenia kadry Policji w zakresie analiz Business Intelligence (BI) i raportowania.
2. Szkolenie zostanie zorganizowane dla osób wytypowanych przez Zamawiającego dla każdego rodzaju szkolenia z podziałem na:
   2.1. Szkolenie dla administratorów z zakresu nowej wersji systemu operacyjnego – 48 osób z podziałem na:
   - KGP i KSP- 8 osób
   - KWP/ SP/CSP – po 2 osoby z każdej jednostki Policji;
   2.2. Szkolenie dla administratorów z zakresu nowej wersji bazy danych – 48 osób z podziałem na:
   - KGP i KSP- 8 osób
   - KWP/ /SP/CSP – po 2 osoby z każdej jednostki Policji;
   2.3. Szkolenie dla administratorów z zakresu rozwiązania HA i DR – 48 osób z podziałem na:
   - KGP i KSP- 8 osób
   - KWP//SP/CSP – po 2 osoby z każdej jednostki Policji;
   2.4. Szkolenie dla administratorów z zakresu usługi katalogowej – 48 osób z podziałem na:
   - KGP i KSP- 8 osób
   - KWP/ SP/CSP – po 2 osoby z każdej jednostki Policji;
   2.5. Szkolenie dla administratorów z zakresu audytu i bezpieczeństwa danych – 48 osób z podziałem na:
   - KGP i KSP- 8 osób
   - KWP/ SP/CSP – po 2 osoby z każdej jednostki Policji;
   2.6. Szkolenie dla administratorów z zakresu procedur eksploatacyjnych – 48 osób z podziałem na:
   - KGP i KSP- 8 osób
   - KWP/ SP/CSP – po 2 osoby z każdej jednostki Policji;
   2.7. Szkolenie dla administratorów z zakresu podstaw analizy i raportowanie BI i języka R – 10 osób z podziałem na:
   - KGP- 10 osób
   2.8. Szkolenie dla administratorów z zakresu MS SQL, T/SQL – 10 osób z podziałem na:
   - KGP- 10 osób
   2.9. Szkolenie dla użytkowników z zakresu podstaw analiz i raportowania BI z uwzględnieniem specyfiki merytorycznej modułów składających się na SWOP – 220 osób z podziałem na:
   - KGP- 10 osób
   - KWP/KSP /SP/CSP – po 10 osób z każdej jednostki Policji;
3. Wykonawca przeprowadzi szkolenie w języku polskim.
4. Zakres szkolenia dla administratorów musi obejmować omówienia wszystkich elementów administracji systemami i bazami, jakie są niezbędne dla prawidłowego nadzoru administracyjnego nad systemem
5. Zakres szkolenia dla administratorów uszczegółowiony jest w ust. 7 zał. nr 1 do Umowy.
6. Czas trwania szkolenia wyniesie minimum 3 dni dla szkoleń dla administratorów systemu.
7. Metoda i forma szkolenia:
   7.1. Forma szkolenia:
   1) Szkolenie stacjonarne w sali szkoleniowej wyposażonej w stanowiska komputerowe,
   2) Jedno stanowisko komputerowe dla 1 słuchacza.
   7.2. Metoda szkolenia:

1) Szkolenie będzie przeprowadzone na bazach szkoleniowych przygotowanych przez Wykonawcę na docelowej wersji oprogramowania (dla wybranej lokalizacji systemu), która zostanie zainstalowana w poszczególnych lokalizacjach Systemu SWOP.

7.3. Realizacja przez Wykonawcę tematów zawartych w planie szkolenia będzie realizowana następująco:
   1) Omówienia tematu przez prowadzącego.
   2) Prezentacja sposobu realizacji danego tematu.
   3) Ćwiczenia wykonywane przez uczestników szkolenia zgodnie z instrukcją i pod nadzorem prelegenta na bazach szkoleniowych udostępnionych przez Wykonawcę.
   4) Podsumowanie poznanych wiadomości praktycznych i teoretycznych w ramach tematu.

8. Wykonawca zobowiązany jest do przeprowadzenia szkolenia zgodnie z zatwierdzonym Harmonogramem realizacji Umowy.
9. Wykonawca zapewni każdemu uczestnikowi szkolenia niezbędne materiały szkoleniowe w języku polskim w formie papierowej oraz w formie elektronicznej w formacie pdf.
10. Wykonawca zapewni, aby szkolenie przeprowadzone zostało przez wykwalifikowaną kadrę szkoleniową, posiadającą wiedzę teoretyczną i praktyczną z zakresu omawianych zagadnień.
11. Przeprowadzenie szkolenia zostanie potwierdzone protokołem zawierającym:
    11.1. nazwę i zakres szkolenia,
    11.2. datę i miejsce przeprowadzenia szkolenia,
    11.3. imienną listę obecności podpisaną przez, osoby uczestniczące w szkoleniu,
    11.4. imię i nazwisko oraz specjalizację osób prowadzących szkolenia.
12. Wykonawca przeprowadzi szkolenia dla użytkowników w następujących terminach:
    12.1. dla administratorów i użytkowników KGP i KSP do zakończenia Etapu I,
    12.2. dla administratorów i użytkowników pozostałych lokalizacji do zakończenia Etapu II,
13. Wykonawca przedstawi Zamawiającemu do akceptacji, w ciągu 40 dni od daty zawarcia Umowy szczegółowy zakres szkoleń dla administratorów i użytkowników.
14. Zamawiający w ciągu 5 (pięciu) Dni roboczych dokona weryfikacji przedstawionych przez Wykonawcę zakresów szkoleń z poszczególnych modułów Oprogramowania dedykowanego.
15. Przekazanie uwag do zakresu szkoleń lub informacji o ich braku, Kierownik Projektu Zamawiającego przekazuje Kierownikowi Projektu po stronie Wykonawcy.
16. W przypadku wniesienia przez Zamawiającego uwag do przedstawionego zakresu szkoleń, Wykonawca przedstawia nowy zakres szkoleń, w terminie 3 dni roboczych od daty przekazania uwag.
17. Zamawiający poddaje weryfikacji nowy zakres szkoleń w ciągu 3 Dni roboczych od daty otrzymania. Weryfikacji podlega tylko zakres szkolenia, do którego Zamawiający zgłosił uwagi.
18. W przypadku nie wniesienia przez Zamawiającego uwag w terminie, o którym mowa w pkt. 14 i 17, zakres szkoleń uważa się za uzgodniony przez Strony Umowy
19. Wykonawca zobowiązany jest do pokrycia kosztów, związanych z wynajęciem odpowiednio wyposażonej sali szkoleniowej (jedno stanowisko komputerowe dla 1 słuchacza), kosztów zakwaterowania i wyżywienia (napoje, przekąski oraz minimum jeden gorący posiłek) .
20. Lista osób, które będą uczestniczyły w szkoleniach, będzie przekazana przez Kierownika Projektu ze strony Zamawiającego do Kierownika Projektu Wykonawcy najpóźniej na 4 dni robocze przed planowaną datą szkoleń.
21. W trakcie każdego dnia szkoleń uczestnicy szkolenia będą podpisywali listę obecności.
22. Przeprowadzenie szkolenia zostanie odebrane poprzez podpisanie Protokołu Odbioru Szkolenia, którego wzór stanowi Załącznik nr 9 do Umowy. Do protokołu z przeprowadzonych szkoleń dołączona zostanie imienna lista osób uczestniczących w szkoleniach z podpisami uczestników w każdym dniu szkoleń oraz lista potwierdzająca odebranie przez uczestników szkolenia imiennych zaświadczeń potwierdzających ich udział w szkoleniach.
23. Kopie imiennych zaświadczeń dla uczestników szkoleń potwierdzających ich udział w szkoleniu, zostaną przekazane przez Kierownika Projektu po stronie Wykonawcy do Kierownika Projektu po stronie Zamawiającego drogą elektroniczną w formacie pdf.

24. Szkolenia uznaje się za zrealizowane przez Wykonawcę również w przypadku, gdy z przyczyn nieleżących po stronie Wykonawcy, liczba osób uczestniczących w szkoleniach będzie mniejsza od liczby osób określonych w Umowie.
25. Nieobecność zgłoszonego pracownika w trakcie szkoleń nie upoważnia Zamawiającego do żądania przeprowadzenia ponownego szkolenia. Zamawiający ma prawo do zastąpienia zgłoszonego i nieobecnego pracownika na szkoleniu innym pracownikiem w trakcie szkolenia, bez wstrzymywania szkolenia.
26. W przypadku gdy w trakcie realizacji szkoleń wystąpią okoliczności uniemożliwiające jego normalne kontynuowanie, Wykonawca zobowiązany jest do zorganizowania nieprzeprowadzonej części szkolenia na własny koszt, w innym terminie, uzgodnionym z Kierownikiem Projektu Zamawiającego.

Załącznik nr 4
do Umowy nr ...../14/BŁiI/17/DG/PMP

Wymagania w zakresie dokumentacji

1. Zamawiający wymaga, by Wykonawca przygotował Dokumentację dla modernizacji Systemu SWOP.
2. Wersje robocze Dokumentacji, które będą podlegały odbiorowi, Kierownik Projektu po stronie Wykonawcy będzie przekazywał drogą elektroniczną do Kierownika Projektu po stronie Zamawiającego.
3. Dokumentacja, zostanie odebrana protokołem odbioru dokumentacji, podpisanym przez komisję powołaną do odbioru przedmiotu Umowy.
4. Dokumentacja, obejmować będzie:
   4.1. Dokumentację projektową wdrożenia.
   4.2. Dokumentację powykonawczą,
   4.3. Dokumentację administratora,
   4.4. Dokumentację użytkownika.
   4.5. Procedury
   4.6. Scenariusze testowe
5. Zamawiający wymaga:
   5.1. Sporządzenia i dostarczenia Dokumentacji w terminach określonych w Harmonogramie realizacji przedmiotu Umowy, opracowanym w trybie i na zasadach określonych w Umowie.
   5.2. Wysokiej jakości wykonania aktualizacji Dokumentacji z uwzględnieniem:
      a. czytelnej i zrozumiałej struktury zarówno poszczególnych dokumentów jak i wszystkich elementów aktualizowanej dokumentacji ;
      b. zachowania jednolitych zasad (standardów) przy tworzeniu wszystkich elementów aktualizowanej dokumentacji (w tym fragmentów tego samego dokumentu);
      c. kompletności tzn. jednoznacznego i wyczerpującego przedstawienia wszystkich zagadnień w odniesieniu do aktualizacji dokumentacji systemu;
      d. przyjęcia jednolitej i spójnej struktury przy tworzeniu zarówno poszczególnych aktualizowanych dokumentów jak i całej aktualizowanej dokumentacji oraz zachowania jednolitej formy i sposobu prezentacji treści.
   5.3. Przekazania Zamawiającemu tj. Komendzie Głównej Policji Dokumentacji, o której mowa w pkt.4 dla każdego etapu w języku polskim, w jednobrzmiących egzemplarzach, po jednym dla każdej jednostki organizacyjnej, w formie drukowanej oraz wersji elektronicznej (płyta CD) w niezabezpieczonym formacie MS Word – DOC i Adobe Acrobat – PDF.
6. Szczegółowa procedura odbioru dokumentacji została opisana w Załączniku nr 6 - Zasady odbioru przedmiotu Umowy.

Załącznik nr 5
do Umowy nr ...../14/BŁiI/17/DG/PMP

SPECYFIKACJA ILOŚCIOWO-CENOWA.

Lp.	Opis	Ilość	Cena jedn. netto /zł./	VAT 23%	Cena jedn. brutto/zł./	Wartość netto /zł./	Wartość brutto/zł./
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
Wartość przedmiotu Umowy:							

Załącznik nr 6
do Umowy nr ...../14/BŁiI/17/DG/PMP

Zasady realizacji Umowy i odbioru przedmiotu Umowy

I. Słownik pojęć

1. **Odbiór przedmiotu Umowy**- zespół czynności dokonywanych przez Strony w celu weryfikacji zrealizowania przez Wykonawcę Umowy, przeprowadzony zgodnie z procedurą odbiorów określoną w odpowiednich załącznikach do Umowy;
2. **Przypadek testowy** – pojedyncza funkcjonalność, która jest testowana w ramach testów akceptacyjnych;
3. **Plan Testów akceptacyjnych** - dokument, w którym zostały opisane wszystkie przypadki testowe do wykonania w ramach testów akceptacyjnych w formie scenariuszy przypadków testowych, który będzie podstawą do dokonania odbioru jakościowego przedmiotu Umowy;
4. **Scenariusz testów akceptacyjnych** - składa się z scenariuszy przypadków testowych;
5. **Scenariusz przypadku testowego** – opis realizacji przypadku testowego zawierający następujące elementy: opis celu przypadku testowego, opisane kroki przypadku testowego, opisany spodziewany rezultat wykonania kroków przypadku testowego;
6. **Testy akceptacyjne** składają się z przypadków testowych;
7. **Dzień Roboczy** - oznacza każdy dzień tygodnia za wyjątkiem sobót, niedziel i dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.

II. Realizacja Umowy.

1. Realizacja Umowy będzie przebiegała w dwóch etapach.

1.1. **Etap I** - Wdrożenie pilotażowe w Komendzie Głównej Policji i Komendzie Stołecznej Policji w terminie wskazanym w § 4 ust. 2 pkt. 1) Umowy, obejmujące następujące produkty:

- 1.1.1. Opracowanie projektu realizacji Etapu I
- 1.1.2. Dostawę sprzętu do KGP i KSP,
- 1.1.3. Instalację na dostarczonym sprzęcie oprogramowania,
- 1.1.4. Konfigurację urządzeń,
- 1.1.5. Uruchomienie usługi katalogowej,
- 1.1.6. Uruchomienie modułu centralnego zarządzania infrastruktura serwerową,
- 1.1.7. Uruchomienie centralnej platformy raportowo-analitycznej (BI),
- 1.1.8. Przeprowadzenie szkoleń,
- 1.1.9. Migrację serwerów i baz danych,
- 1.1.10. Przeprowadzenie testów wydajności, niezawodności oraz poprawności działania SWOP na nowym środowisku,
- 1.1.11. Przeprowadzenie testów platformy raportowo-analitycznej (BI),
- 1.1.12. Przeprowadzenie testów zarządzania infrastrukturą serwerową,
- 1.1.13. Opracowanie dokumentacji i procedur.

1.2. **Etap II** – Wdrożenie eksploatacyjne we wszystkich lokalizacjach Systemu SWOP w terminie wskazanym w § 4 ust. 2 pkt. 2) Umowy, obejmujące następujące produkty:

- 1.2.1. Opracowanie projektu realizacji Etapu II
- 1.2.2. Dostawę sprzętu do pozostałych lokalizacji,
- 1.2.3. Instalację na dostarczonym sprzęcie oprogramowania,
- 1.2.4. Konfigurację urządzeń,
- 1.2.5. Przeprowadzenie szkoleń,
- 1.2.6. Migrację serwerów i baz danych

1.2.7. Przeprowadzenie testów wydajności, niezawodności oraz poprawności działania SWOP na nowym środowisku,
1.2.8. Przeprowadzenie testów zarządzania infrastrukturą serwerową,
1.2.9. Opracowanie dokumentacji i procedur.

III. Zasady ogólne odbioru przedmiotu Umowy.

1. Odbiór przedmiotu Umowy zostanie potwierdzony podpisaniem w Komendzie Głównej Policji przez Komisję powołaną przez Komendanta Głównego Policji, przy udziale upoważnionego przedstawiciela lub przedstawicieli Wykonawcy protokołu odbioru produktu, którego wzór stanowi Załącznik nr 13 do Umowy. Podpisany bez zastrzeżeń protokół odbioru produktu jest podstawą do wystawienia faktury VAT przez Wykonawcę.
2. Odbiór produktów w lokalizacjach innych niż Komenda Główna Policji, zostanie dokonany przez komisję powołaną przez kierowników jednostek organizacyjnych Policji (JOP).
3. Odbiór produktów etapu przedmiotu Umowy zostanie potwierdzony podpisaniem przez komisję, o której mowa w pkt. 1 i upoważnionego przedstawiciela lub przedstawicieli Wykonawcy protokołu odbioru etapu, którego wzór stanowi Załącznik nr 12 do Umowy.
4. Odbiorowi podlegają produkty obejmujące:
   4.1. Sprzęt – odbiór ilościowy.
   4.2. Dokumentację - odbiór dokumentacji.
   4.3. Usługi instalacji, konfiguracji, migracji– odbiór jakościowy, dokonany na podstawie testów akceptacyjnych, scenariuszy i przypadków testowych oraz dokumentacji związanej z konfiguracją serwerów i oprogramowania na potrzeby Systemu SWOP.
   4.4. Szkolenia dla administratorów i użytkowników – odbiór szkoleń.
   4.5. Konsultacje specjalistyczne – odbiór usługi
5. O przygotowaniu przedmiotu Umowy lub część Umowy do odbioru, o którym mowa w pkt. 1-4 Wykonawca powiadomi faksem Wydział Zarzadzania Projektami BŁiI KGP na numer (022) 60-158-73 lub na wskazany w Umowie adres e-mail Zamawiającego, podając:
   5.1. numer niniejszej Umowy,
   5.2. planowaną datę odbioru,
   5.3. ilość i przedmiot odbioru (numery seryjne produktu jeśli dotyczy).
6. Zamawiający ma obowiązek przystąpienia do odbioru przedmiotu Umowy o którym mowa w pkt. 1-4 w ciągu 5 Dni Roboczych od otrzymania od Wykonawcy zgłoszenia gotowości do odbioru, o którym mowa w ust. 5
7. Wszystkie czynności związane z odbiorami muszą się zakończyć w terminie realizacji Umowy określonym w § 4 ust. 1 Umowy.
8. Protokoły, o których mowa w ust. 1 - 4 zostaną sporządzone w 4 (czterech) jednobrzmiących egzemplarzach z których 3 (trzy) egzemplarze otrzymuje Zamawiający i odpowiednio 1 (jeden) egzemplarz otrzymuje Wykonawca

IV. Szczegółowe zasady odbioru przedmiotu Umowy.

1. Odbiór ilościowy.

1.1. Odbiorowi ilościowemu podlega: sprzęt, licencje i nośniki oprogramowania dostarczone przez Wykonawcę.
1.2. W celu przeprowadzenia odbioru Wykonawca w ramach Umowy dokona dostawy przedmiotu odbioru na własny koszt, do wskazanych przez Zamawiającego pomieszczeń w lokalizacjach objętych wdrożeniem w godz. 8:30-15:00. Pomieszczenie zostanie wskazane przez Zamawiającego nie później niż na 1 Dzień Roboczy przed planowaną datą odbioru.
1.3. Czynności kontrolne prowadzone w ramach odbioru ilościowego będą polegały na potwierdzeniu zgodności dostawy z nazwą i ilością określoną w wykazie ilościowym.
1.4. Wykonawca będzie odpowiedzialny za rozpakowanie dostarczonego produktu, o ile będzie to konieczne podczas odbioru.

1.5. Dokonanie odbioru bez uwag zostanie potwierdzone podpisaniem bez zastrzeżeń Protokołu Odbioru ilościowego stanowiącego Załącznik nr 7 do Umowy.
1.6. Wykonawca dostarczy dokumenty licencyjne na oprogramowanie zgodnie ze swoim szablonem. Dokumenty Licencyjne powinny zawierać informację o Wystawcy Licencji, Odbiorcy Licencji oraz ilości użytkowników, numerze Umowy i nazwie oprogramowania i Dokumentacji, której dotyczy licencja.
1.7. Potwierdzeniem dostarczenia ilości licencji dostępowych dla użytkowników będzie dokument wystawiony przez Wykonawcę, potwierdzający prawo użytkowania przez Policję ilości licencji wymaganych przez Zamawiającego.
1.8. O przygotowaniu do odbioru ilościowego Wykonawca powiadomi Zamawiającego w sposób, o którym mowa w Rozdz. III pkt.5.
1.9. Zamawiający przystąpi do odbioru ilościowego w terminie określonym w Rozdz. III pkt. 6.

2. Odbiór szkoleń.

2.1. Odbiór całości szkoleń dla administratorów i użytkowników przeprowadzonych przez Wykonawcę, zostanie dokonany w Komendzie Głównej Policji przez komisję Zamawiającego powołaną Decyzją Komendanta Głównego Policji i potwierdzony podpisaniem protokołu odbioru szkoleń stanowiącym Załącznik nr 10 do Umowy.
2.2. Odbiór dla każdego rodzaju szkolenia zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego oraz Wykonawcy protokołu odbioru szkolenia nr, którego wzór określa Załącznik nr 9 do Umowy
2.3. Szkolenia, o których mowa w pkt. 2.2 mogą być przeprowadzane z podziałem na etapy i lokalizacje.
2.4. Odbioru szkoleń, o których mowa w pkt. 2.2 dokonują Kierownicy Projektu Stron Umowy lub osoby przez nich upoważnione.
2.5. Odbiór szkoleń dla użytkowników i administratorów z zakresu każdego z etapów, będzie przeprowadzony odrębnie.
2.6. Szkolenia zostaną odebrane przez Zamawiającego przy udziale Wykonawcy zgodnie z wymaganiami i zasadami określonymi w Załączniku nr 3 do Umowy .
2.7. Załącznikami do protokołu, o którym mowa w pkt. 2.1 będą protokoły odbioru poszczególnych szkoleń przeprowadzonych przez Wykonawcę, których wzór określa Załącznik nr 9 do Umowy.
2.8. O przygotowaniu do odbioru szkoleń Wykonawca powiadomi Zamawiającego w sposób, o którym mowa w Rozdz. III pkt.5.
2.9. Zamawiający przystąpi do odbioru szkoleń w terminie określonym w Rozdz. III pkt. 6.

3. Odbiór Dokumentacji.

3.1. Odbiór Dokumentacji dla modernizacji systemu SWOP zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego oraz Wykonawcy protokołów odbioru dokumentacji, których wzór stanowi załącznik nr 8 do Umowy.
3.2. Dokumenty składające się na Dokumentację modernizacji systemu SWOP przygotowane przez Wykonawcę są akceptowane przez Zamawiającego zgodnie z procedurą opisaną w kolejnych punktach.
3.3. Kierownik Projektu Wykonawcy przekazuje wersje elektroniczne Dokumentację Systemu SWOP do Kierownika Projektu Zamawiającego, w celu jej weryfikacji. Wersja zaakceptowana przez Zamawiającego na zasadach określonych w niniejszym Załączniku zostanie dostarczona przez Wykonawcę w formie, o której mowa w Załączniku nr 4 pkt.5.
3.4. Dokumenty zostaną poddane weryfikacji przez Zamawiającego w ciągu dziesięciu (10) Dni Roboczych od daty przekazania dokumentu przez Wykonawcę do Zamawiającego.
3.5. Zamawiający ma możliwość zgłoszenia uwag do dokumentu w formie elektronicznej do Wykonawcy, które zostaną przekazane jednorazowo dla danej wersji Dokumentacji.

3.6. Uwagi Zamawiającego do dokumentacji Kierownik Projektu po stronie Zamawiającego przekazuje Kierownikowi Projektu po stronie Wykonawcy. Kierownicy Projektu Stron Umowy ustalają nową datę dostarczenia poprawionej wersji dokumentacji.

3.7. Dla poprawionej wersji dokumentacji kroki niniejszej procedury zostają powtórzone, przy czym okres ponownej weryfikacji dokumentacji przez Zamawiającego wynosi trzy (3) Dni Robocze. Weryfikacja poprawionej dokumentacji dotyczy tylko tych elementów Dokumentacji, do których były zgłaszane uwagi.

3.8. Akceptacja przez Zamawiającego wersji dokumentacji przedstawionej przez Wykonawcę, staje się podstawą do wszczęcia procedury odbioru Dokumentacji, o której mowa w Rozdziale III pkt.4 i 5.

3.9. Jeżeli Zamawiający nie zgłosi żadnych uwag do dokumentów w okresie jej weryfikacji, dokumenty zostaną uznane za zaakceptowane przez obie Strony Umowy, co staje się podstawą do wszczęcia procedury, o której mowa w pkt.3.8.

3.10. O przygotowaniu do odbioru dokumentacji Wykonawca powiadomi Zamawiającego w sposób, o którym mowa w Rozdz. III pkt.5.

3.11. Zamawiający przystąpi do odbioru dokumentacji w terminie określonym w Rozdz. III pkt. 6.

4. Odbiór jakościowy.

4.1. Odbiór jakościowy będzie przeprowadzony w Komendzie Głównej Policji w Warszawie i lokalizacjach objętych wdrożeniem.

4.2. Celem czynności kontrolnych prowadzonych w ramach odbioru jakościowego jest sprawdzenie wszystkich wymagań funkcjonalnych dostarczonego produktu i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.

4.3. Podstawą dokonania odbioru jakościowego jest przeprowadzenie z pozytywnym skutkiem testów akceptacyjnych przewidzianych dla poszczególnych etapów według Planu Testów akceptacyjnych oraz scenariuszy i przypadków testowych.

4.4. Plan testów akceptacyjnych zawierający scenariusze testowe i przypadki testowe dla modernizacji systemu SWOP Wykonawca przekazuje Kierownikowi Projektu Zamawiającego zgodnie z Harmonogramem realizacji Umowy.

4.5. Plan Testów akceptacyjnych oraz scenariusze i przypadki testowe zostaną poddane weryfikacji przez Zamawiającego w ciągu pięciu (5) Dni Roboczych od daty ich przekazania przez Wykonawcę do Zamawiającego.

4.6. Zamawiający zgłasza do Wykonawcy swoje uwagi w formie elektronicznej , które zostaną przekazane przez Kierownika Projektu Zamawiającego jednorazowo dla każdej wersji.

4.7. Jeżeli Zamawiający nie zgłosi żadnych uwag do planu testów lub do przypadków i scenariuszy testowych w okresie ich weryfikacji przez Zamawiającego, zostaną one uznane za zaakceptowane przez obie Strony.

4.8. Jeżeli Zamawiający zgłosi uwagi do planu testów w „okresie akceptacji" zdefiniowanym powyżej, Kierownik Projektu Wykonawcy określa czas ustosunkowania się Wykonawcy do uwag. Następnie Kierownicy Projektu ustalają datę dostarczenia zmodyfikowanych wersji planu testów

4.9. Dla zmodyfikowanej wersji planu testów oraz scenariuszy i przypadków testowych kroki niniejszej procedury zostają powtórzone, przy czym okres weryfikacji wynosi trzy (3) Dni Robocze. Weryfikacji przez Zamawiającego poddawane są tylko te elementy planu testów oraz scenariuszy i przypadków testowych, które wynikają z uwag zgłoszonych przez Zamawiającego w okresie weryfikacji.

4.10. Do wykonania odbioru jakościowego będą wykorzystane dokumenty zaakceptowane przez Zamawiającego.

4.11. O przygotowaniu do odbioru jakościowego Wykonawca powiadomi Zamawiającego w sposób, o którym mowa w Rozdz. III pkt.5.

4.12. Zamawiający przystąpi do odbioru jakościowego w terminie określonym w Rozdz. III pkt. 6.
4.13. Pozytywny wynik odbioru jakościowego zostanie potwierdzony podpisaniem przez komisje powołane do odbioru przedmiotu Umowy i Wykonawcę protokołem odbioru jakościowego, który stanowi Załącznik nr 11 do Umowy.

5. Odbiór produktu

6.1. Odbiór produktu kończy procedurę odbioru przedmiotu Umowy.
6.2. Protokół Odbioru Produktu może zostać podpisany po dokonaniu przez Komisję powołaną przez Zamawiającego i przedstawicieli Wykonawcy odbioru każdego etapu Umowy i stanowi Załącznik nr 13 do Umowy.
6.3. Protokoły odbioru ilościowego, jakościowego, dokumentacji, szkoleń oraz usługi będą stanowiły załączniki do protokołu odbioru Etapu, który stanowi Załącznik nr 12 do Umowy.

Załącznik nr 7
do Umowy nr ...../14/BŁiI/17/DG/PMP

PROTOKÓŁ ODBIORU ILOŚCIOWEGO .....

do Umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:
.....
Data dokonania odbioru:
.....
Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)
Ze strony Zamawiającego:
.....
(nazwa i adres)

Na podstawie czynności odbiorczych, przeprowadzonych w ramach Umowy Komisja do odbioru przedmiotu zamówienia, powołana na mocy.....z dnia ..... r. potwierdza kompletność i wymagane w Umowie ilości dostarczonych przez Wykonawcę licencji serwerowych oprogramowania:

Lp.	Przedmiot odbioru ilościowego	Ilość	Uwagi

Uwagi:.....
.....
Podpisy Komisji do odbioru przedmiotu zamówienia:

Przewodniczący:
.....
Członkowie:
1. .....
2. .....
3.....
(Członkowie komisji Zamawiającego)

1.....
2.....
3.....
(upoważnieni przedstawiciele Wykonawcy)

Załącznik nr 8
do Umowy nr ...../14/BŁiI/17/DG/PMP

PROTOKÓŁ ODBIORU DOKUMENTACJI
do umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:
.....

Data dokonania odbioru:
.....

Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(imię i nazwisko osoby upoważnionej do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)
W ramach czynności odbiorczych, przeprowadzonych w ramach umowy nr ..... z dnia.....r. na...../nazwa projektu/....., Komisja powołana na mocy.....z dnia ..... r.:

Potwierdza kompletność dostarczonej przez Wykonawcę dokumentacji:

Lp.	Nazwa Dokumentacji	Wersja	Ilość	Uwagi

Potwierdza wymagany w umowie poziom jakości dostarczonej dokumentacji:
- Zgodne*
- Niezgodne z umową*

Opis stwierdzonych niezgodności/rozbieżności .....

Uwagi:.....
.....
Podpisy Komisji do odbioru przedmiotu zamówienia:
Przewodniczący:
.....

Członkowie:

1. .....
2. .....
3.....
(Członkowie Komisji Zamawiającego)

1. .....
2. .....
3. .....
(upoważniony Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 9
do Umowy nr ...../14/BŁiL/17/DG/PMP

PROTOKOŁU ODBIORU SZKOLENIA nr .....
do Umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....
w ramach „.....”

Miejsce dokonania odbioru:

.....

Data dokonania odbioru:

.....

Ze strony Wykonawcy:

.....

(nazwa i adres)

.....

(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:

.....

(nazwa i adres)

.....

(osoba upoważniona do udziału w odbiorze)

1. Termin szkolenia – .....
2. Ilość godzin szkolenia: - .....
3. Liczba uczestników szkolenia:.....
4. Przedmiot i zakres szkolenia:
   .....

Uwagi:.....
.....

Przedstawiciel Zamawiającego

.....

Przedstawiciel Wykonawcy

.....

Załącznik nr 10
do Umowy nr ...../14/BŁiI/17/DG/PMP

PROTOKÓŁ ODBIORU SZKOLEŃ
dla „.....”
do Umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:

.....

Data dokonania odbioru:

.....

Ze strony Wykonawcy:

.....
(nazwa i adres)

.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:

.....
(nazwa i adres)

.....
(osoba upoważniona do udziału w odbiorze)

1. Termin szkolenia ....
2. Ilość godzin szkolenia: .....
3. Liczba uczestników szkolenia:.....
4. Przedmiot i zakres szkolenia:

_____/tytuł szkolenia/_____

Na podstawie czynności odbiorczych, przeprowadzonych w ramach Umowy Komisja do odbioru przedmiotu zamówienia, powołana na mocy.....z dnia ..... r. potwierdza zgodność przeprowadzonego szkolenia z warunkami Umowy.

Załączniki:

1. Harmonogram szkoleń
2. Protokoły z odbioru szkolenia w ramach „.....” z listami obecności uczestników szkolenia oraz listą poświadczeń odbioru certyfikatów przez uczestników szkolenia.

Podpisy Komisji do odbioru przedmiotu zamówienia:

Przewodniczący:

.....

Członkowie:

1.	1.....
2.	2.....
3.....	3.....
(Członkowie komisji Zamawiającego)	(upoważnieni przedstawiciele Wykonawcy)

Załącznik nr 11
do Umowy nr ...../14/BŁiI/17/DG/PMP

PROTOKÓŁ ODBIORU JAKOŚCIOWEGO
„.....”

do Umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:
.....
Data dokonania odbioru:
.....
Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

W ramach odbioru jakościowego, przeprowadzonego w ramach Umowy nr ..... z dnia.....
na...../nazwa projektu/.....,
Komisja powołana na mocy.....z dnia ..... r. przeprowadziła czynności kontrolne na podstawie zatwierdzonego przez Strony Umowy Planu Testów Akceptacyjnych, scenariuszy i przypadków testowych i potwierdza zgodność jakości dostarczonego produktu z parametrami/funkcjonalnością zawartymi w opisie przedmiotu Umowy.

Wynik odbioru jakościowego:
- Pozytywny*
- Negatywny*

Uwagi:.....
.....
.....
.....
Podpisy Komisji do odbioru przedmiotu zamówienia:
Przewodniczący:
.....
Członkowie:

1.	1.....
2.	2.....
3.....	3.....
(Członkowie komisji Zamawiającego)	(upoważnieni przedstawiciele Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 12
do Umowy nr ...../14/BŁiI/17/DG/PMP

PROTOKÓŁ ODBIORU ETAPU NR .....

do Umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:
.....
Data dokonania odbioru:
.....
Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

na mocy ..... nr ..... z dnia.....

Komisja potwierdza/nie potwierdza* wykonanie Etapu nr ..... zgodne z warunkami zawartymi w Umowie na podstawie niżej wymienionych Protokołów Odbioru zadań/produktów, które stanowią załączniki do niniejszego protokołu::

1. .....
2. .....
3. .....

Uwagi**:.....
.....
.....

Podpisy Komisji do odbioru przedmiotu zamówienia:
Przewodniczący:
.....
Członkowie:

1.	1.....
2.	2.....
3.....	3.....
(Członkowie komisji Zamawiającego)	(upoważnieni przedstawiciele Wykonawcy)

*niewłaściwe skreślić
** wypełnić w przypadku negatywnego odbioru, podając jego szczegółowe przyczyny

Załącznik nr 13
do Umowy nr ...../14/BŁiI/17/DG/PMP

PROTOKÓŁ ODBIORU PRODUKTU

do Umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:
.....
Data dokonania odbioru:
.....
Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Komisja do obioru przedmiotu zamówienia w składzie:

1.....
2. .....
3. .....

na podstawie przeprowadzonych czynności kontrolnych oraz Protokołów odbioru jakościowego / odbioru ilościowego / odbioru szkolenia / odbioru dokumentacji * potwierdza wykonanie zamówienia zgodne z warunkami zawartymi w umowie.

Uwagi.....
.....
.....

Podpisy Komisji do odbioru przedmiotu zamówienia:

Przewodniczący:
.....
Członkowie:

1.....	1. .....
2.	2. .....
3.	3. .....
(Członkowie komisji Zamawiającego)	(upoważnieni Przedstawiciele Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 14
do Umowy nr ...../14/BŁiI/17/DG/PMP

.....
(imię i nazwisko)

.....

.....
(miejsce zatrudnienia)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

1. Stwierdzam własnoręcznym podpisem, że zobowiązuję się do nie przekazywania, nie ujawniania oraz nie wykorzystywania bez zgody Dyrektora Biura Łączności i Informatyki KGP wiadomości udostępnionych przez pracowników i funkcjonariuszy BŁiI KGP oraz uzyskanych w związku z wykonywaniem Umowy nr ... zawartej w .....r. pomiędzy Komendantem Głównym Policji a firmą ....., a nie podlegających wykluczeniom na podstawie poniższych zapisów:
2. jeżeli informacja została ujawniona publicznie przez stronę, będącą właścicielem informacji chronionej;
3. jeżeli ujawnienia informacji żąda sąd lub organ ścigania w toku prowadzonych czynności na podstawie stosownych przepisów;
4. jeżeli właściciel informacji chronionej wyrazi na to uprzednio zgodę pisemną;
5. jeżeli informacja została uzyskana od osób trzecich bez naruszenia prawnych zobowiązań o poufności informacji.

.....
(data i podpis składającego oświadczenie)