Znak sprawy: **ZP-4/DTP/2013** *Załącznik Nr 5.1 do SIWZ*

DATA TECHNO PARK

Dostawa infrastruktury informatycznej i oprogramowania na potrzeby tworzenia i rozwoju nowoczesnych e-usług i aplikacji on-line oraz ich świadczenia w sektorze ochrony zdrowia wraz z wdrożeniem na terenie Medycznego Centrum Przetwarzania Danych DTP Sp. z o.o. we Wrocławiu

# Zadanie 1: Stworzenie warunków do tworzenia i rozwoju nowoczesnych usług informatycznych w sektorze ochrony zdrowia

# 1 Wprowadzenie

Dokument określa szczegółowy przedmiot zamówienia oraz tryb dostarczenia produktów. Stanowi podstawę rozliczenia pracy Wykonawcy i główny dokument nadzorczy przy:

- Projektowaniu rozwiązania przez Wykonawcę przy współudziale Zamawiającego
- Wykonaniu rozwiązania przez Wykonawcę
- Odbieraniu rozwiązania od Wykonawcy przez Zamawiającego

## 1.1.Struktura dokumentów

Dokument składa się z wydzielonych logicznych części ułożonych w następującym porządku:

1. Wprowadzenie – opisuje podstawy związane z aparatem pojęciowym niezbędnym do prawidłowej percepcji dokumentu
2. Zakres dokumentu – opisuje zakres zamówienia w postaci zwięzłej listy produktów
3. Kontekst biznesowy – opisuje cel przedsięwzięcia i podstawowe usługi dla klientów
4. Aplikacje biznesowe i infrastrukturalne – opisuje listę oraz szczegółowy zakres podstawowych elementów oprogramowania do wytworzenia i/lub dostarczenia
5. Infrastruktura techniczna – opisuje elementy infrastruktury programowej (oprogramowanie standardowe) oraz infrastruktury technicznej (sprzętowej, fizycznej, sieciowej i storage)
6. Wymagania ogólne – istotne postanowienia związane z trybem dostarczenia produktów oraz wymagań wspólnych
7. Katalogi usługi i interfejsów – indykatywna lista wszystkich usług na poziomie aplikacyjnym oraz technicznym oraz interfejsów

## 1.2.Metamodel

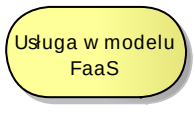
Metamodel opisuje w jaki sposób należy interpretować pojęcia, relacje i diagramy opisane w niniejszym dokumencie (wspólnie nazywane modelem).

Metamodel dotyczy elementów diagramów oraz wymagań.

### Diagramy

Diagram jest graficzną reprezentacją istotnych z punktu widzenia niniejszego Zamówienia rozwiązań. Znaczenie zastosowanych diagramów oraz ich elementów są w ogólności zgodne ze specyfikacją ArchiMate 2.0[1].

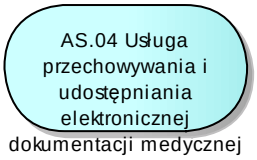
Do najważniejszych wykorzystanych konstrukcji należą:




Usługa biznesowa – usługa występująca na linii Data Techno Park – klient. Usługa biznesowa jest to usługa, która stanowi element oferty handlowej Data Techno Park. Wiąże się z wykorzystaniem systemów informatycznych, ale również innych formalno-organizacyjnych zadań.

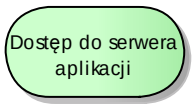
[1] https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12480

Wypełnienie elementu metamodelu kolorem żółtym oznacza, że jest to element warstwy biznesowej.



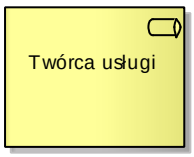

Usługa aplikacyjna – usługa udostępniana przez system informatyczny. Istotna z punktu widzenia usługi biznesowej czynność realizowana przez system informatyczny. Posiada interfejs dostępu (graficzny lub programistyczny).

Wypełnienie elementu metamodelu kolorem błękitnym oznacza, że jest to element warstwy systemów informatycznych.

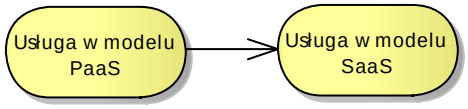



Usługa techniczna – usługa udostępniana przez infrastrukturę sprzętową lub programową. Jest niezbędna w celu świadczenia usług wyższego poziomu (aplikacyjnych i biznesowych).

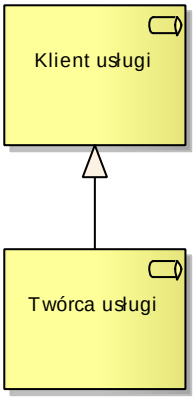
Wypełnienie elementu metamodelu kolorem zielonym oznacza, że jest to element warstwy technicznej.



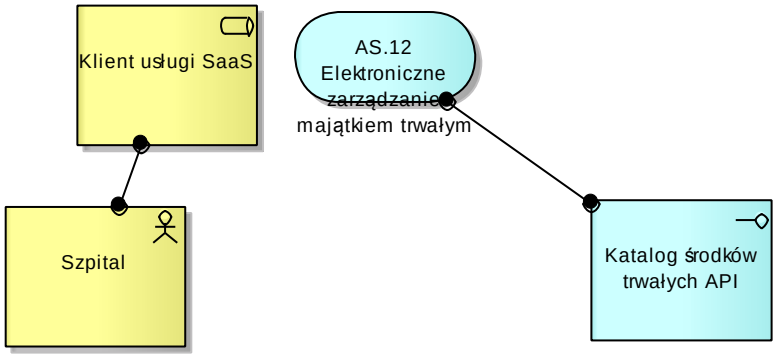

Rola – odpowiedzialność za wykonywanie określonych czynności. Rolą są przyjmowane przez aktorów (np. szpital).



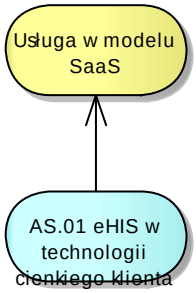

Relacja usedBy (wykorzystywana przez), tutaj: Usługa w modelu PaaS jest wykorzystywana przez Usługą w modelu SaaS, co oznacza, że Usługa w modelu SaaS wymaga usługi w modelu PaaS lub inaczej Usługa w modelu SaaS jest zależna od Usługa w modelu PaaS.



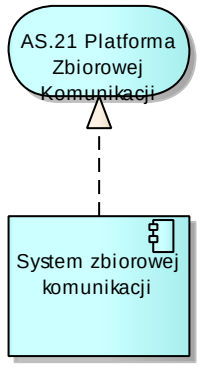

Relacja dziedziczenia (specjalizacja) oznacza, że Rola Twórca usługi jest specjalizacją Roli Klient usługi.



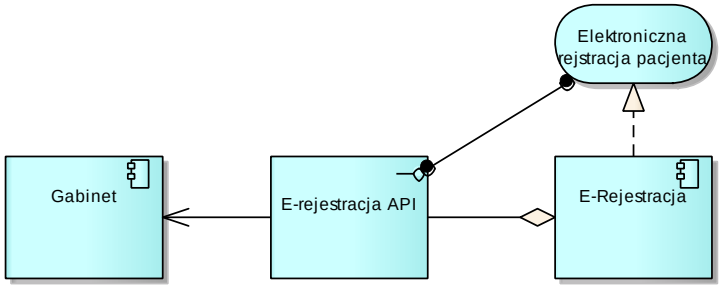

Relacja przydzielenia (ang. assignment) oznacza, że Szpital występuje w roli Klienta usługi SaaS oraz Usługa AS.12 jest reprezentowana przez Interfejs Katalog środków trwałych API.




Relacja usedBy (wykorzystywany przez) pomiędzy usługą biznesową a usługą aplikacyjną oznacza, że usługa aplikacyjna musi być świadczona jako dany typ usługi biznesowej. W tym przypadku oznacza to, że usługa AS.01 jest usługą świadczoną w modelu SaaS.




Relacja realise (realizacji) oznacza, że usługa jest realizowana przez komponent. W tym przypadku, usługa aplikacyjna AS.21 jest realizowana przez komponent aplikacyjny System zbiorowej komunikacji. Inaczej mówiąc, dany komponent realizuje daną usługę (System zbiorowej komunikacji realizuje usługę AS.21).




Często powtarzający się układ relacji pomiędzy integrującymi się aplikacjami – aplikacja Gabinet wykorzystuje (integruje się z) interfejsem E-rejestracja API, który jest częścią (relacja agregacji) aplikacji E-Rejestracja, która to aplikacja realizuje usługę Elektroniczna rejestracja pacjenta (a sama usługa jest reprezentowana przez interfejs E-rejestracja API).

## Wymagania

Każde wymaganie posiada unikalny identyfikator, krótką nazwę charakteryzującą czego dotyczy wymaganie oraz treść.

Przyjęto iż wymagania dla usług są wymaganiami (głównie pozafunkcjonalnymi), które odnoszą się do wszystkich lub większości systemów i aplikacji, i nie są w związku z tym umieszczane w kontekście poszczególnych elementów.

Wymagania techniczne (głównie funkcjonalne) umieszczone są w kontekście poszczególnych elementów. Wymagania te są współdzielone pomiędzy elementami. Oznacza, to że to samo wymaganie (o tym samym identyfikatorze i treści) definiujące określoną funkcjonalność, umieszczane jest w kontekście każdego z elementów, który uczestniczy musi je realizować.

W celu jednoznacznej identyfikacji wymagań przyjęto następujące zasady.

Identyfikatory wymagań budowane są w oparciu o:

- Skrót elementu, którego dotyczy, np. BEZP (wymagania z obszaru infrastrukturalnego Bezpieczeństwo)
- Nr kolejny wymagania w kontekście danej grupy (numerowanie rozpoczyna się od nowa dla kolejnej grupy)

## 1.3.Słownik zastosowanych terminów

W dokumencie zastosowano powtarzające się terminy o następującym znaczeniu:

| Termin | Znaczenie |
|---|---|
| Domyślny serwer aplikacyjny | Serwer aplikacyjny spełniający wymagania określone w sekcji 5.6.2. Zakłada daleko idącą integrację środowisk aplikacyjnych. |
| Domyślne środowisko bazodanowe | Baza danych spełniająca wymagania określone w sekcji 5.5.1 zakładająca wysoki stopień konsolidacji struktur bazodanowych (instancji oraz schematów). |

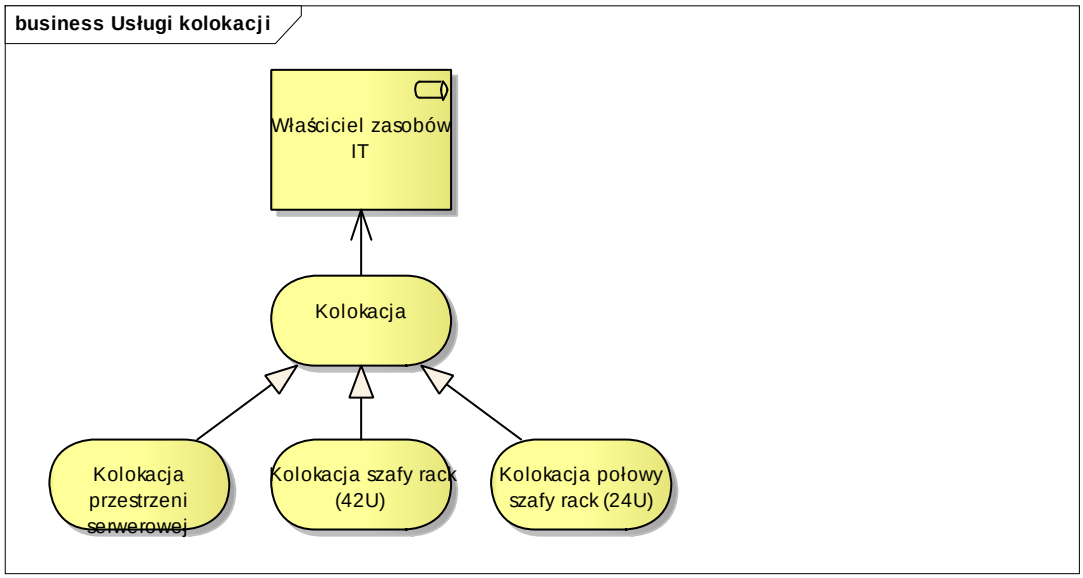
Dla pozostałych pojęć stosuje się zapisy Słownika pojęć, stanowiący Załącznik nr 16 do SIWZ.

# 2 Kontekst biznesowy

Celem Data Techno Park-u jest uruchomienie przy ulicy Borowskiej we Wrocławiu centrum przetwarzania danych w modelu cloud computing, w którym świadczy się usługi na rzecz klientów. Usługa stanowi element oferty Zamawiającego i podlega działalności handlowej oraz operacyjnej. Zakres i warunki świadczenia usług normowane są umową zawieraną pomiędzy Data Techno Park a klientem usługi.

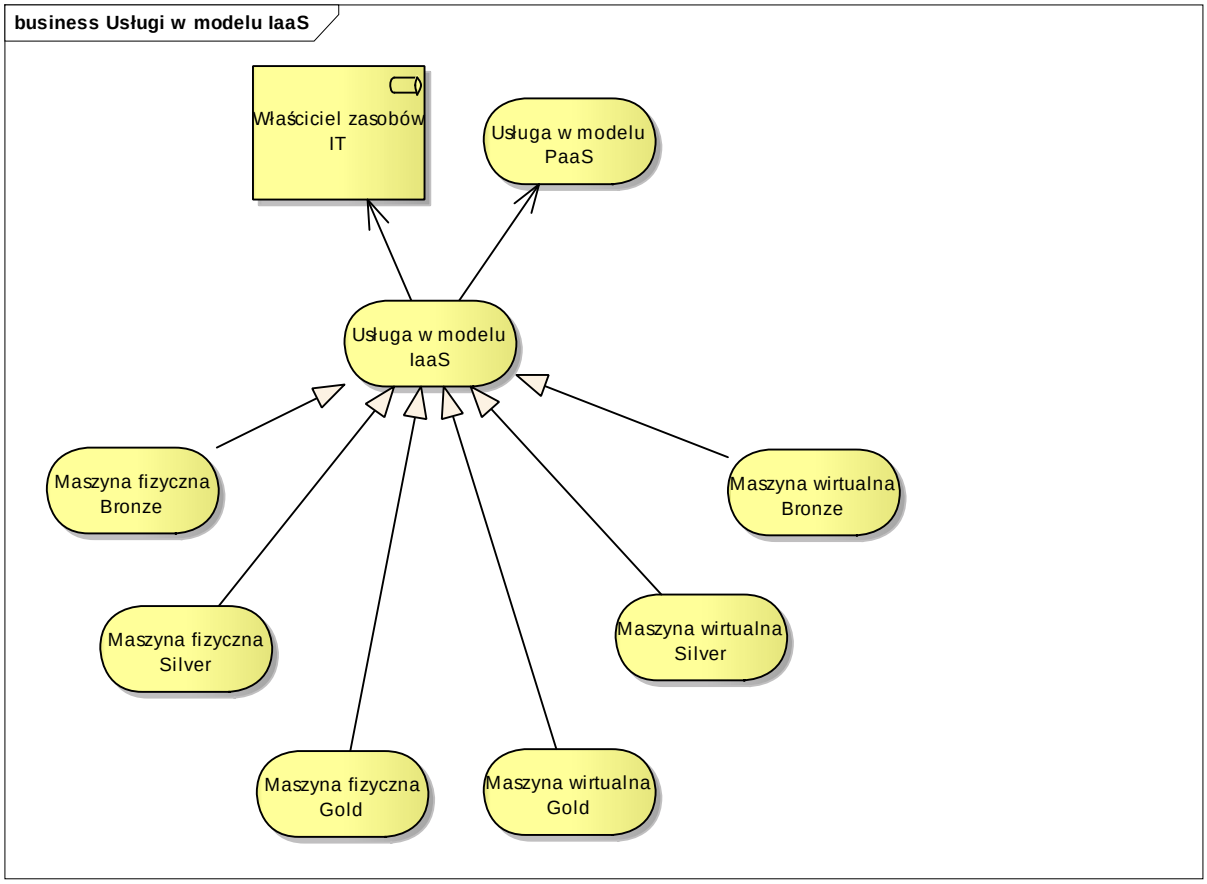
W realizowanym centrum świadczone będą następujące usługi:

- Usługi kolokacji – grupa usług polegających na umieszczeniu sprzętu technicznego oraz oprogramowania w serwerowni Data Techno Park.



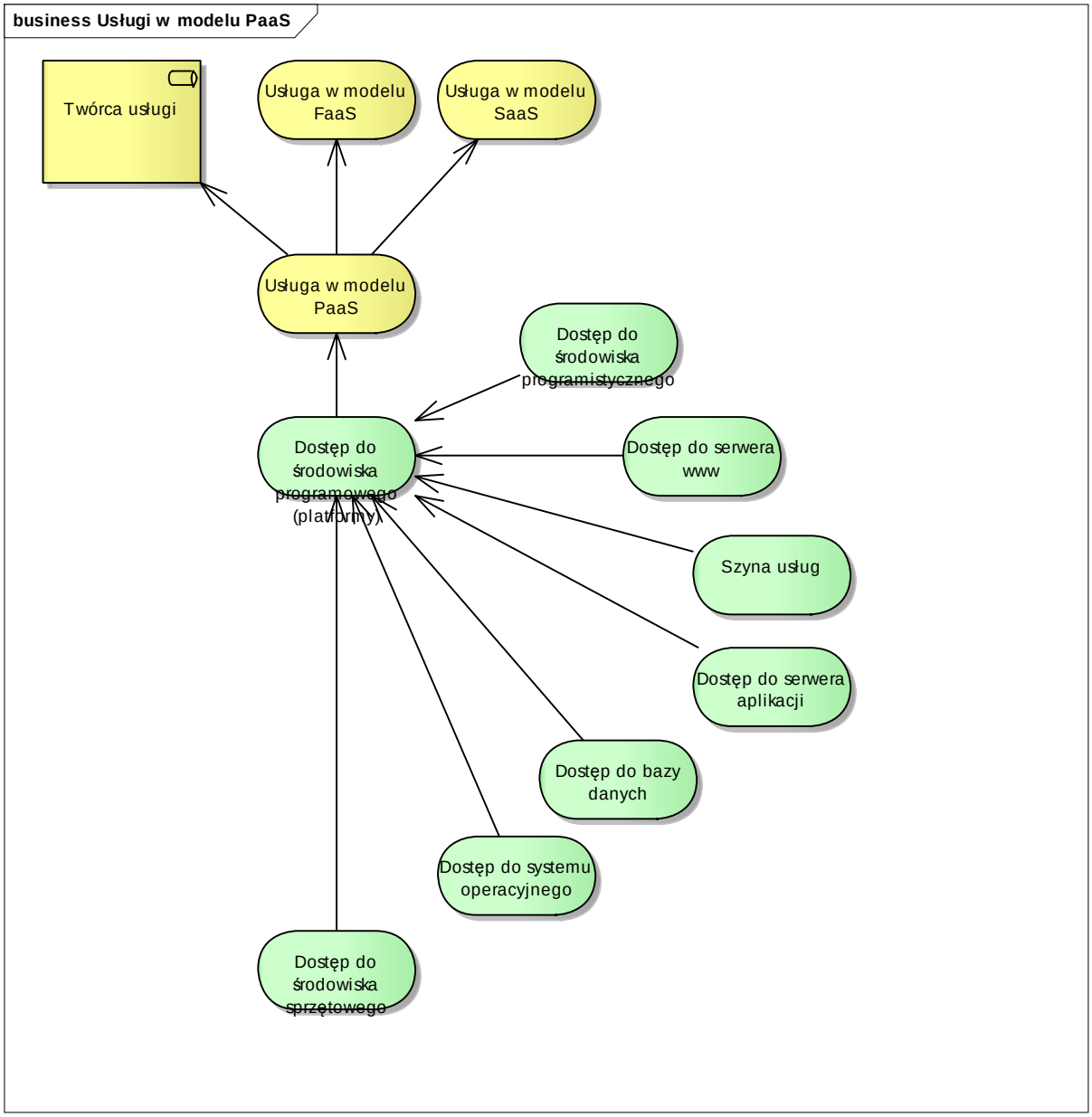

Rysunek 1 Usługi kolokacji

- Usługi w modelu IaaS (ang. Infrastructure as a Service) – grupa usług polegających na świadczeniu dostępu do sprzętu technicznego w zakresie mocy obliczeniowej oraz przestrzeni dyskowej




Rysunek 2 Usługi IaaS

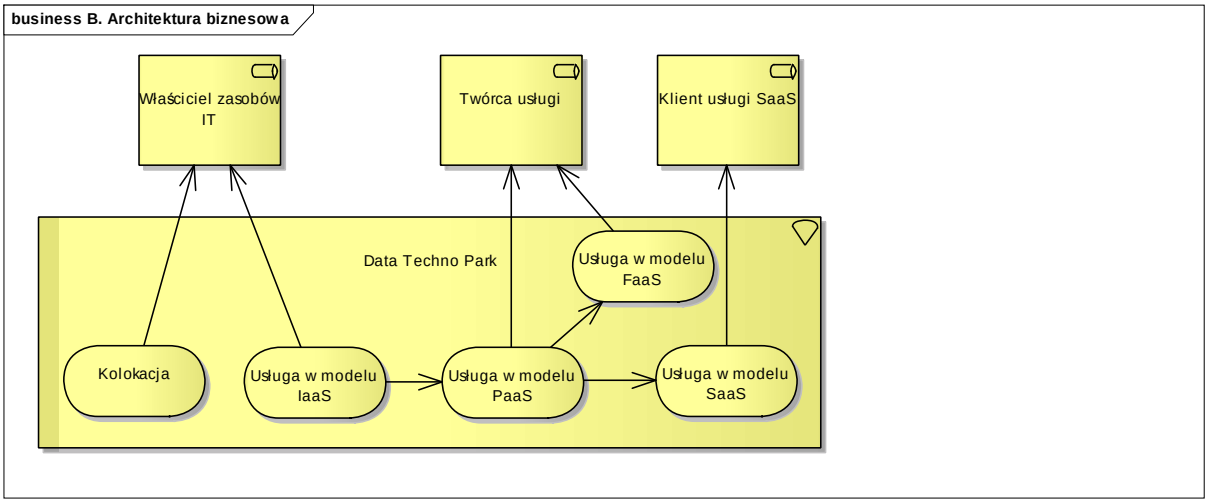
- Usługi w modelu PaaS (ang. Platform as a Service) – grupa usług polegających na świadczeniu dostępu do sprzętu technicznego oraz oprogramowania standardowego pozwalającego na tworzenie aplikacji dedykowanych. Usługi w modelu PaaS wykorzystują usługi w modelu IaaS.




Rysunek 3 Usługi PaaS

- Usługi w modelu FaaS (ang. Framework as a Service) – grupa usług polegających na świadczeniu dostępu do platformy programowej, w której istnieją wstępnie przygotowane narzędzia pozwalające znacząco skrócić czas wytwarzania aplikacji dedykowanych dla branży medycznej. Nie są to jeszcze gotowe aplikacje, które można oferować klientom. Grupa usług FaaS pozwala wykorzystać moduły, które zawierają najczęściej powtarzające się funkcje systemów dla branży medycznej, umożliwiając twórcom usług medycznych koncentrację na funkcjach stanowiących o ich przewadze konkurencyjnej. Usługi w modelu FaaS wykorzystują usługi w modelu IaaS oraz PaaS (w zakresie dostępu do sprzętu oraz oprogramowania standardowego).
- Usługi w modelu SaaS (ang. Software as a Service) – grupa usług polegających na świadczeniu usług na rzecz klientów końcowych (np. szpitali, przychodni) w formie dostosowanych i gotowych aplikacji. Klient usługi SaaS kupuje dostęp do gotowej aplikacji. Usługi w modelu

SaaS wykorzystują usługi w modelu IaaS oraz PaaS (w zakresie dostępu do sprzętu oraz oprogramowania standardowego).

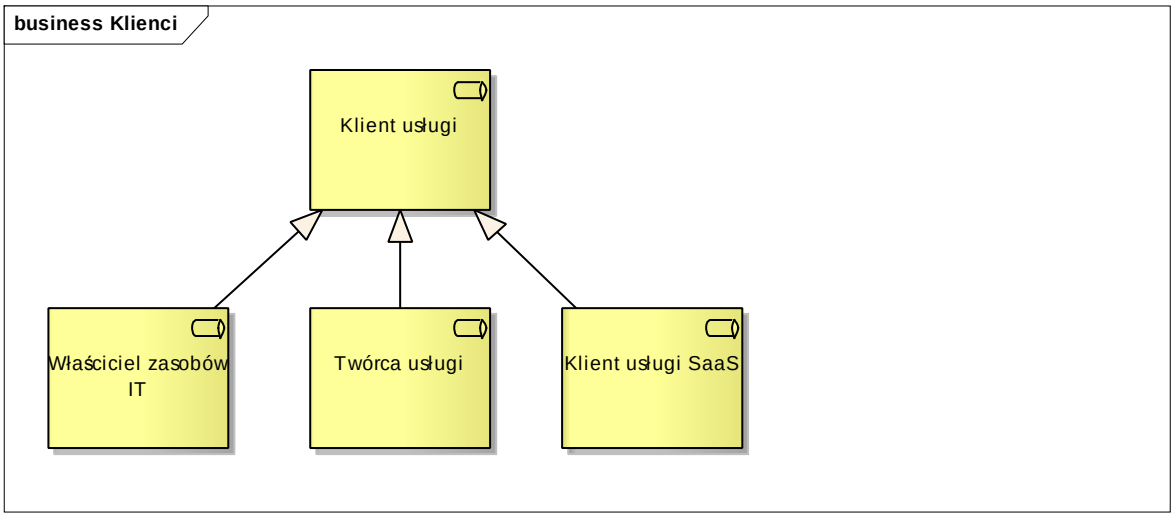



Rysunek 4 Zestawienie typów usług biznesowych, które docelowo będą świadczone przez Zamawiającego

Klientami usług kolokacji i IaaS są ogólnie pojmowani właściciele zasobów IT, np. serwerów lub aplikacji własnych, którzy potrzebują przestrzeni, mocy obliczeniowej lub przestrzeni dyskowej do budowy lub utrzymania własnych zasobów IT.

Klientami usług PaaS oraz FaaS są twórcy usług, którzy mogą koncentrować się na budowie aplikacji otrzymując od Zamawiającego niezbędne zasoby infrastrukturalne i aplikacyjne (w postaci platformy).

Klientami usług SaaS są podmioty rynku medycznego, administracji samorządowej lub dowolnej innej branży, dla których Partnerzy Data Techno Parku świadczą komercyjnie usługi IT.




Rysunek 5 Klienci usług Data Techno Park

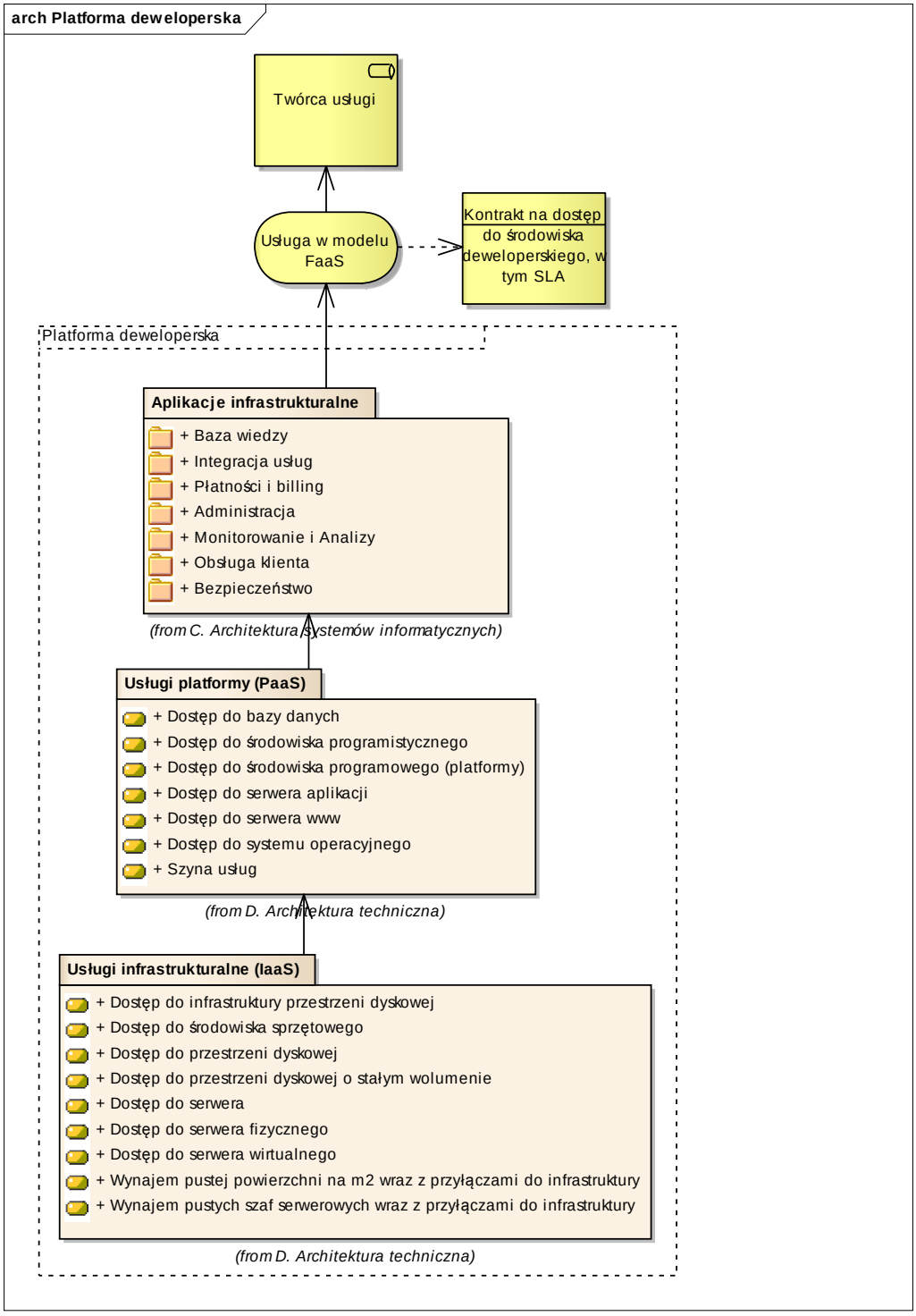
Podział odpowiedzialności w zależności od typu świadczonej usługi reguluje model referencyjny PCI DSS v2 Cloud Computing Guidelines, gdzie Data Techno Park jest podmiotem CSP (ang. *Cloud Service Provider*). Zgodność z PCI DSS v2 oznacza, że:

- W modelu IaaS DTP ponosi odpowiedzialność za prawidłowe świadczenie usług na następujących poziomach:
  - Środowisko fizyczne (ang. physical facility)
  - Sieć (ang. network)
  - Fizyczny sprzęt do przechowywania danych (ang. data storage)
  - Fizyczny sprzęt dostarczający CPU i pamięć (ang. processing and memory)
  - Platforma nadzorująca wirtualizacją (ang. hypervisor) – w przypadku, gdy stosuje się warstwę wirtualizacji
- W modelu PaaS DTP ponosi odpowiedzialność za prawidłowe świadczenie usług na poziomach objętych modelem IaaS oraz dodatkowo:
  - Wirtualna infrastruktura sieciowa (ang. virtual network infrastructure)
  - Maszyna wirtualna (ang. virtual machine) – maszyna wirtualna dedykowana dla klienta
  - System operacyjny (ang. operating system)
- W modelu FaaS DTP ponosi odpowiedzialność za prawidłowe świadczenie usług na poziomach objętych modelem PaaS oraz dodatkowo:
  - Środowisko uruchomieniowe (ang. solution stack), np. środowisko .Net lub środowisko Java, w tym serwer aplikacji i serwer bazodanowy
  - Aplikacje (ang. applications) – aplikacje wchodzące w skład Platformy (aplikacje infrastrukturalne i biznesowe)
  - Część interfejsów (ang. interfaces) – część interfejsów, głównie API związana z wykorzystaniem aplikacji przez inną aplikację
- W modelu SaaS DTP ponosi odpowiedzialność za prawidłowe świadczenie usług na poziomach objętych modelem PaaS oraz dodatkowo:
  - Środowisko uruchomieniowe (ang. solution stack), np. środowisko .Net lub środowisko Java, w tym serwer aplikacji i serwer bazodanowy
  - Aplikacje (ang. applications) – dedykowane dla klienta aplikacje biznesowe
  - Część interfejsów (ang. interfaces) – część interfejsów API i GUI związana z wykorzystaniem aplikacji przez klienta

Realizacja założonych celów biznesowych wymaga wsparcia ze strony systemów informatycznych oraz odpowiednich technologii programowych i sprzętowych. W przełożeniu na usługi należy rozumieć, że usługi biznesowe wymagają wsparcia usług aplikacyjnych (aplikacji) oraz usług technicznych.

# 3 Zakres zamówienia

Zakres niniejszego Zamówienia to dostarczenie Platformy Deweloperskiej, która pozwala świadczyć usługi w modelu FaaS (Framework as a Service). Platforma Deweloperska składa się z aplikacji infrastrukturalnych (sekcja 4) oraz z usług technicznych, tj. usług platformy udostępnianych w modelu PaaS oraz usług infrastrukturalnych udostępnianych w modelu IaaS (zwanych łącznie infrastrukturą techniczną – sekcja 5).




Rysunek 6 Zakres zamówienia

W ramach dostarczenia Platformy Deweloperskiej Wykonawca jest zobowiązany do wykonania następujących czynności:

- Wykonanie analizy przedwdrożeniowej;
- Dostarczenia, zainstalowania oraz skonfigurowania niezbędnej infrastruktury informatycznej;
- Dostarczenia, wdrożenia oraz parametryzacji oprogramowania;
- Przeprowadzenia testów akceptacyjnych;
- Przeprowadzenia instruktaży stanowiskowych dla przedstawicieli Zamawiającego;
- Zapewnienia asysty stanowiskowej dla przedstawicieli Zamawiającego na etapie wdrażania oraz w okresie gwarancji;
- Przekazania Zamawiającemu pełnej dokumentacji technicznej dostarczonej infrastruktury informatycznej i oprogramowania;
- Udzielenia gwarancji w okresie wskazanym w formularzu oferty (co najmniej 3-letniej).

# 4 Aplikacje infrastrukturalne

Aplikacja infrastrukturalna to typ aplikacji, która jest świadczona pośrednio na rzecz klienta i pełni rolę pomocniczą dla oferowanych usług biznesowych. Dla klientów, którzy korzystać będą z usług aplikacje infrastrukturalne pełnią rolę drugorzędną w stosunku do aplikacji biznesowych, nie mniej jednak stanowią spójną platformę w tworzeniu usług oraz ujednoliceniu procesu ich świadczenia.

Przedstawione w niniejszym rozdziale aplikacje infrastrukturalne wspierają świadczenie wszystkich rodzajów usług biznesowych. Ich wykorzystanie jest obligatoryjne, a wszelkie odstępstwa stanowią odstępstwo architektoniczne i podlegają oddzielnej ścieżce decyzyjnej.

## 4.1 Platforma BI

Platforma BI (Business Intelligence) składa się z dedykowanego systemu bazodanowego oraz zbioru kostek przeznaczonych do analizy zjawisk medycznych.

System bazodanowy (SBD) musi spełniać poniższe wymagania poprzez wbudowane mechanizmy.

| ID wymagania | Opis wymagania |
|---|---|
| BI.1. | Rozwiązanie musi pozwalać na wykorzystanie SBD, jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Rozwiązanie powinno zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. |
| BI.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. |
| BI.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. |
| BI.4. | Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. |
| BI.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. |
| BI.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). |
| BI.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). |
| BI.8. | Możliwość dodawania procesorów bez restartu systemu - SBD powinien umożliwiać dodanie procesora do systemu, bez konieczności restartu silnika bazy danych. |
| BI.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. |
| BI.10. | Możliwość dodawania pamięci bez restartu systemu - SBD powinien umożliwiać dodanie pamięci do systemu bez konieczności restartu silnika bazy danych. |
| BI.11. | SBD musi umożliwiać tworzenie klastrów niezawodnościowych. Powinien również umożliwiać tworzenie klastrów niezawodnościowych, których węzły znajdują się w różnych podsieciach komputerowych. |
| BI.12. | Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych |

| | |
|---|---|
| | między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:<br>a) bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),<br>b) niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),<br>c) klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,<br>d) czas przełączenia na system zapasowy poniżej 10 sekund,<br>e) brak limitu odległości miedzy systemami (dopuszczalne są tylko limity w minimalnej wymaganej przepustowości łącza oraz limity wynikające z opóźnień na łączu),<br>f) kompresja danych przesyłanych między serwerem podstawowym i zapasowym (w celu minimalizacji obciążenie sieci),<br>g) 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). |
| BI.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. |
| BI.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. |
| BI.15. | 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. |
| BI.16. | 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. |
| BI.17. | Możliwość zastosowania reguł bezpieczeństwa obowiązujących u klienta usługi - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory oraz mechanizmem bezpieczeństwa stosowanym domyślnie w Data Techno Park. |
| BI.18. | 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. |
| BI.19. | Ograniczenie użycia zasobów – SBD powinien posiadać wbudowany mechanizm ograniczający wykorzystanie zasobów systemu operacyjnego (% wykorzystania czasu procesora, % wykorzystania pamięci). 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). |
| BI.20. | 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:<br>a) odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),<br>b) wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),<br>c) para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy). |
| BI.21. | 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. |
| BI.22. | 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. |
| BI.23. | 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. |
| BI.24. | Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:<br>a) udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,<br>b) udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,<br>c) udostępniać język zapytań do struktur XML,<br>d) udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),<br>e) udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań. |
| BI.25. | 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:<br>a) zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,<br>b) 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.,<br>c) obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,<br>d) 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.). |
| BI.26. | 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). |
| BI.27. | 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. |
| BI.28. | 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. |
| BI.29. | 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. |
| BI.30. | 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). |
| BI.31. | 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. |
| BI.32. | Indeksowanie podzbioru danych w tabeli - SBD powinien umożliwiać tworzenie indeksów na podzbiorze danych z tabeli określonym poprzez wyrażenie filtrujące. |
| BI.33. | 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. |
| BI.34. | 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. |
| BI.35. | 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. |
| BI.36. | Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych. |
| BI.37. | 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. |
| BI.38. | 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.:<br>a) mechanizm debuggowania tworzonego rozwiązania,<br>b) mechanizm stawiania „pułapek" (breakpoints),<br>c) mechanizm logowania do pliku wykonywanych przez transformację operacji,<br>d) możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),<br>e) możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)<br>f) mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),<br>g) mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),<br>h) 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,<br>i) mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych,<br>j) możliwość integracji z transakcjami bazy danych SBD, także rozproszonymi bez potrzeby pisania kodu. |
| BI.39. | 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. |
| BI.40. | 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). |
| BI.41. | 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). |
| BI.42. | Narzędzia do zarządzania jakością danych - SBD powinien mieć wbudowane mechanizmy do zarządzania jakością danych w organizacji. W ramach tych funkcji powinien:<br>a) udostępniać funkcje do profilowania danych (analiza i raporty dotyczące jakości danych),<br>b) udostępniać funkcje do deduplikacji danych, |

| | |
|---|---|
| | c) określać stopień poprawności wartości atrybutu i w przypadku błędnej wartości sugerować wartość poprawną do akceptacji przez użytkownika,<br>d) umożliwiać definiowanie osobnych reguł czyszczenia dla wybranych domen (typów atrybutów),<br>e) 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),<br>f) pozwalać na ręczną korektę nieprawidłowych danych w dedykowanej aplikacji (bez konieczności programowania),<br>g) 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,<br>h) przechowywać reguły walidujące i oceniające jakość danych w dedykowanej bazie danych (bazie wiedzy),<br>i) umożliwiać uzupełnianie i rozszerzanie bazy wiedzy o dane referencyjne pochodzące z systemów zewnętrznych,<br>j) 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,<br>k) 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). |
| BI.43. | Możliwość zarządzania centralnymi słownikami danych - SBD powinien dostarczać narzędzia do przechowywania i zarządzania centralnym słownikiem danych (Master Data Management - MDM). System MDM powinien:<br>a) udostępniać narzędzia do wprowadzania, modyfikacji i wyszukiwania danych w słownikach,<br>b) umożliwiać wersjonowanie danych (śledzenie zmian wprowadzonych przez użytkowników z możliwością ich cofnięcia do wybranej wersji),<br>c) udostępniać mechanizm tworzenia i uruchamiania reguł walidujących poprawność danych w słownikach,<br>d) udostępniać narzędzia do administracji i kontroli uprawnień dostępu do danych w MDM,<br>e) udostępniać zestaw bibliotek (API programistyczne) z funkcjonalnościami MDM do wykorzystania w aplikacjach użytkownika,<br>f) umożliwiać eksport danych zgromadzonych w systemie MDM,<br>g) umożliwiać zarządzanie danymi podstawowymi z poziomu programu Microsoft Excel. |
| BI.44. | Wbudowany system analityczny powinien posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych. |
| BI.45. | 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). |
| BI.46. | Wbudowany system analityczny powinien obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta). |
| BI.47. | Wbudowany system analityczny powinien udostępniać mechanizm zapisu danych przez użytkownika do kostek wielowymiarowych. |
| BI.48. | 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. |
| BI.49. | 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. |
| BI.50. | 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. |
| BI.51. | 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. |
| BI.52. | 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). |
| BI.53. | 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. |
| BI.54. | 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. |
| BI.55. | Wbudowany system analityczny powinien zapewniać mechanizmy dynamicznego security (każdy z użytkowników modelu powinien widzieć tylko swoje dane). |
| BI.56. | 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. |
| BI.57. | 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. |
| BI.58. | 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). |
| BI.59. | 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. |
| BI.60. | System analityczny powinien pozwalać na dodawanie własnych algorytmów oraz modułów wizualizacji modeli Data Mining. |
| BI.61. | 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. |
| BI.62. | System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą |

| | |
|---|---|
| | przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania powinien obsługiwać:<br>a) raporty parametryzowane,<br>b) cache raportów (generacja raportów bez dostępu do źródła danych),<br>c) cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),<br>d) współdzielenie predefiniowanych zapytań do źródeł danych,<br>e) wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),<br>f) możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,<br>g) możliwość wizualizacji wskaźników KPI,<br>h) możliwość wizualizacji danych w postaci obiektów sparkline. |
| BI.63. | Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services). |
| BI.64. | Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel (od wersji 1997 do 2010), Microsoft Word (od wersji 1997 do 2010), HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach. |
| BI.65. | 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. |
| BI.66. | SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja) do dynamicznej listy odbiorców (pobieranej z bazy danych np. zapytaniem SQL). |
| BI.67. | Wbudowany system raportowania powinien posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT. |
| BI.68. | 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. |
| BI.69. | Platforma BI będzie posiadała kostki umożliwiające wykonanie następujących analiz:<br>1. Koszty procesu medycznego - zawiera analizę kosztów składających się na leczenie pacjentów<br>2. Przychody procesu medycznego - zawiera analizę przychodów uzyskanych przy leczeniu pacjentów<br>3. Umowy - obejmuje analizę stanu i realizacji kontraktów |
| BI.70. | Platforma BI musi być dostarczona razem z licencjami na silnik bazodanowy w liczbie pozwalającej na jego uruchomienie na 2 serwerach 8 rdzeniowych (razem 16 rdzeni). |
| BI.71. | Platforma BI musi być dostarczona razem z licencjami na system operacyjny w wersji serwerowej w liczbie pozwalającej na jego uruchomienie na 4 CPU. |

## 4.2 Portal wielofunkcyjny

Portal wielofunkcyjny (PW) intranet i internet muszą realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy:

| ID wymagania | Opis wymagania |
|---|---|
| PW.1 | Portal wielofunkcyjny musi umożliwiać publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych |
| PW.2 | Portal wielofunkcyjny musi umożliwiać zarządzanie strukturą portalu i treściami WWW |
| PW.3 | Portal wielofunkcyjny musi umożliwiać uczestnictwo Internautów w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści |

| | |
|---|---|
| PW.4 | Portal wielofunkcyjny musi umożliwiać udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej |
| PW.5 | Portal wielofunkcyjny musi umożliwiać udostępnienie formularzy elektronicznych. |
| PW.6 | Portal wielofunkcyjny musi umożliwiać tworzenie repozytoriów wzorów dokumentów. |
| PW.7 | Portal wielofunkcyjny musi umożliwiać tworzenie repozytoriów dokumentów |
| PW.8 | Portal wielofunkcyjny musi umożliwiać wspólną, bezpieczną pracę nad dokumentami |
| PW.9 | Portal wielofunkcyjny musi umożliwiać wersjonowanie dokumentów (dla wersji roboczych) |
| PW.10 | Portal wielofunkcyjny musi umożliwiać organizację pracy grupowej |
| PW.11 | Portal wielofunkcyjny musi umożliwiać wyszukiwanie treści |
| PW.12 | Portal wielofunkcyjny musi umożliwiać dostęp do danych w relacyjnych bazach danych |
| PW.13 | Portal wielofunkcyjny musi umożliwiać analizy danych wraz z graficzną prezentacją danych |
| PW.14 | Portal wielofunkcyjny musi umożliwiać wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning). |
| PW.15 | Serwery Portalu wielofunkcyjnego muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie. |
| PW.16 | Portal wielofunkcyjny musi udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów. |

Portal wielofunkcyjny musi posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

| ID wymagania | Opis wymagania |
|---|---|
| PW.17 | Interfejs użytkownika:<br>• Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu).<br>• Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0<br>• Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów<br>• Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego<br>• Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu<br>• Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy). |
| PW.18 | Uwierzytelnianie – wbudowane mechanizmy wspierające uwierzytelnianie na bazie:<br>• Oświadczeń (claim-based authentication) z wykorzystaniem:<br>• Open Authorization 2.0 dla uwierzytelniania aplikacji,<br>• Uwierzytelniania w trybie server-to-server,<br>• SAML<br>• Windows claims<br>• Pojedynczego logowania domenowego (single-sign on),<br>• Na bazie formularzy (Form-based). |
| PW.19 | Projektowanie stron<br>• Wbudowane intuicyjne narzędzia projektowania wyglądu stron,<br>• Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML, |

| | |
|---|---|
| | • Wsparcie dla ASP.NET, Apache, C#, Java i PHP,<br>• Możliwość osadzania elementów iFrame w polach HTML na stronie. |
| PW.20 | Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:<br>• Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili<br>• Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów<br>• Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili<br>• Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony)<br>• Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego<br>• Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services<br>• Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP.<br>• Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych. |
| PW.21 | Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści:<br>• Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania.<br>• Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML)<br>• Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego<br>• Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów<br>• Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte<br>• Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana<br>• Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego |

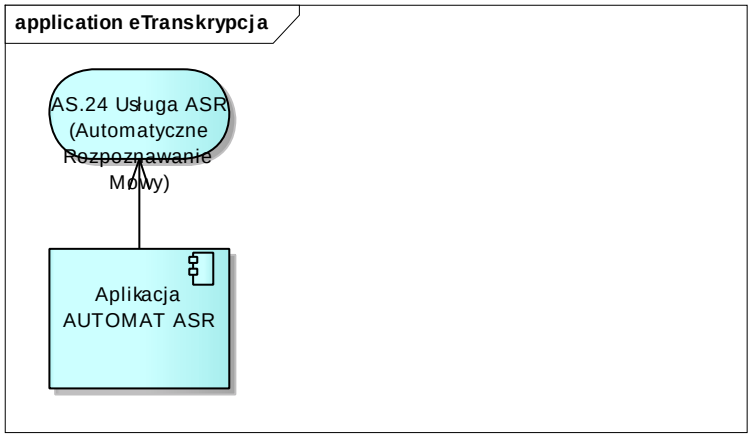
| | |
|---|---|
| | (projekt graficzny i funkcjonalny).<br>• Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo. |
| PW.22 | Organizacja i publikacja treści:<br>• Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.<br>• Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.<br>• Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.<br>• Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię.<br>• Automatyczne generowanie mapy stron portalu.<br>• Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi.<br>• Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.<br>• Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.<br>• Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.<br>• Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.<br>• Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu oraz zapewnienie automatycznego tłumaczenia na wybrane języki. |
| PW.23 | Repozytoria dokumentów:<br>• Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów.<br>• Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa.<br>• Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu.<br>• Możliwość publikacji plików w strukturze katalogów.<br>• Możliwość publikacji materiałów wideo oraz audio.<br>• Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku.<br>• Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów.<br>• Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania.<br>• Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), automatyczna kontrola wersji przy publikacji dokumentów.<br>• Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub |

| | |
|---|---|
| | modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub odrzuceniu.<br>• Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych.<br>• Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów.<br>• Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich.<br>• Możliwość automatyzacji usuwania duplikatów dokumentów. |
| PW.24 | Wyszukiwanie treści:<br>• Pełnotekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice.<br>• Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu<br>• Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji<br>• Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów<br>• Możliwość definiowania słownika słów wykluczonych (często używanych)<br>• Możliwość tworzenia „linków sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania w zależności od słów wpisanych w zapytaniu<br>• Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu.<br>• Przedstawianie w wynikach duplikatów plików<br>• Statystyki wyszukiwanych fraz |
| PW.25 | Administracja intranetem i inne funkcje:<br>• Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych<br>• Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu<br>• Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści<br>• Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu oraz centralnie zarządzanego zbioru metadanych z wyznaczonym administratorem merytorycznym.<br>• Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów,<br>• Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu<br>• Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy<br>• Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń<br>• Funkcjonalność publikowania na portalu formularzy elektronicznych XML i |

| | |
|---|---|
| | przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza.<br>• Mechanizmy wspierające przepływy pracy (workflow) wraz z funkcjonalnością definiowania procesów obiegu dokumentów, integracji przepływów z web-services, wywoływania web-services z poziomu workflow bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu. |
| PW.26 | System musi umożliwiać obsługę procesu związanego z dokumentacją:<br>• Przyspieszenie terminu operacji<br>• Umowa/Aneks na wykonywanie badań na świadczenie usług medycznych (inne niż NFZ, MZ)<br>• Prośba o zawarcie umowy na świadczenia medyczne<br>• Porozumienie w sprawie spłaty zadłużenia<br>• Wstrzymanie dostaw towaru<br>• Zmiana danych kontrahentów<br>• Umowa/Aneks do umowy rezydenckiej- pielęgniarki<br>• Umowa/Aneks do umowy rezydenckiej- lekarze<br>• Umowa/Aneks do umowy rezydenckiej- pozostałe<br>• Umowa Staż/specjalizacja/praktyka/wolontariat<br>• Zapytania ofertowe na świadczenia medyczne<br>• Oferty przetargowe<br>• Postępowanie przetargowe<br>• Przedłużenie terminu związania ofertą<br>• Zapytania do przetargów<br>• Przedłużenie terminu związania ofertą<br>• Zapytania do przetargów<br>• Oferty handlowe<br>• Decyzje zatwierdzające program gospodarki odpadami medycznymi<br>• KRS, Księga Rejestrowa, REGON<br>• Ankiety/udostępnienie danych do prac naukowych - w zakresie pielęgniarek<br>• Ankiety/udostępnienie danych do prac naukowych - w zakresie lekarzy<br>• Ankiety/udostępnienie danych do prac naukowych- pozostałe<br>• Nakaz-wniosek z prokuratury-żądanie wydania rzeczy<br>• Dokumentacja medyczna (pacjent, firma ubezpieczeniowa, ZUS, sąd, prokuratura, policja)<br>• Pisma z Urzędu Miasta i Gminy (potwierdzenie, udostępnienie danych)<br>• Rozłożenie na raty zapłaty za pobyt w szpitalu<br>• Umorzenie opłaty za pobyt w Szpitalu<br>• Nota korygująca/sprzedaż<br>• Oświadczenie o sfinansowaniu leku dla pacjenta<br>• Wycofanie produktu leczniczego<br>• Wnioski na sprowadzenie leku z zagranicy |
| PW.27 | Portal musi być dostarczony razem z licencjami pozwalającymi na jego uruchomienie na 2 serwerach 8 rdzeniowych (razem 16 rdzeni). |
| PW.28 | Portal musi być dostarczony razem z licencjami na system operacyjny w wersji serwerowej w liczbie pozwalającej na jego uruchomienie na 4 CPU. |

## 4.3 ASR (rozpoznawanie mowy)

Usługa umożliwia automatyczne rozpoznawanie mowy (ASR), tj. przetworzenie nagrania (zapisu cyfrowego) do postaci dokumentu tekstowego. Świadczenie usługi wspiera system do rozpoznawania mowy.



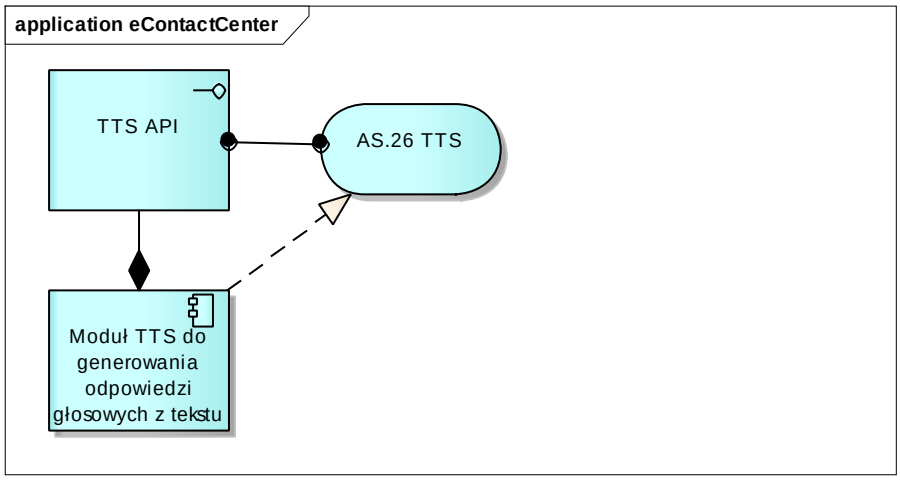

Rysunek 7 Usługa ASR

Wymagania funkcjonalne dla oprogramowania wspierającego świadczenie usługi:

| ID wymagania | Opis wymagania |
|---|---|
| ASR.1. | Usługa musi umożliwiać zapisanie wyników transkrypcji w postaci pliku tekstowego, który opisany zostanie co najmniej następującymi metadanymi:<br>• Odniesienie do źródłowego pliku audio<br>• Dacie oraz godzinie wykonania transkrypcji |
| ASR.2. | Oprogramowanie służy do automatyzacji procesu translacji mowy w języku polskim na tekst. |
| ASR.3. | Zakres rozpoznawanych tekstów obejmuje ogólne słownictwo języka polskiego |
| ASR.4. | Zakres rozpoznawanych tekstów obejmuje branżowe słownictwo medyczne stosowane przez lekarzy w języku polskim (minimum 100 tys. słów) |
| ASR.5. | Oprogramowanie przetwarzać będzie pliki dźwiękowe w formacie VAW (16kHz, 16 bit, mono) |
| ASR.6. | Oprogramowanie zapisywać będzie rozpoznane teksty w formacie „xml" z kodowaniem znaków zgodnie ze standardem UTF-8 |
| ASR.7. | Oprogramowanie musi podawać prawdopodobieństwo, jakie przypisane zostało każdemu rozpoznanemu słowu bądź wyrażeniu. |
| ASR.8. | Oprogramowanie obsługuje wszystkie znaki pisma polskiego w tym ą, ę, ń, dż, dź, ł, ś, ć, ó, ż, ź, cz, sz, rz |
| ASR.9. | Oprogramowanie powinno pozwalać na jednoczesne przetwarzanie co najmniej 160 plików zadań (przetwarzanie 160 plików z nagraniami) |
| ASR.10. | Oprogramowanie powinno zarządzać kolejką rozpoznawania (w przypadku, gdy bieżąca ilość zadań (plików) w trakcie tłumaczenia przekroczy 160. |
| ASR.11. | Oprogramowanie powinno umożliwiać przenoszenie danych (rozpoznanych tekstów) do systemu informatycznego za pomocą ustalonego wcześniej portu TCP/IP i / lub funkcji API |
| ASR.12. | Zapewniana przez oprogramowanie bezbłędność (skuteczność) translacji mowy na tekst powinna być wyższa lub równa 94%. |
| ASR.13. | Definiowanie słowników pozwalających na zamianę tekstu mówionego na ściśle określony zdefiniowany przez użytkownika tekst lub skrót. |
| ASR.14. | Rozpoznawanie (zamiana mowy na tekst), nie może trwać dłużej niż czterokrotność czasu nagrania dźwiękowego dla jednego rdzenia CPU w przypadku słownika 100 000 słów. |
| ASR.15. | Rozpoznawanie mowy ma przebiegać w trybie wsadowym tzn. oprogramowanie przyjmować będzie pliki dźwiękowe za pomocą ustalonego wcześniej portu TCP/IP i / lub funkcji API |
| ASR.16. | Zastępowanie istniejących korpusów i modeli językowych nowymi, zawierającymi nowe słowa lub teksty |
| ASR.17. | Rozwiązanie musi być dostosowane do sytuacji, w której awaria pojedynczego serwera nie może spowodować braku dostępności usługi |

## 4.4 Generator mowy

Usługa musi pozwalać na generowanie odpowiedzi głosowej na podstawie tekstu w języku naturalnym. Świadczenie usługi wspiera system, tzw. generator mowy.




Rysunek 8 Usługa TTS

Wymagania minimalne dla aplikacji wspierającej świadczenie usługi:

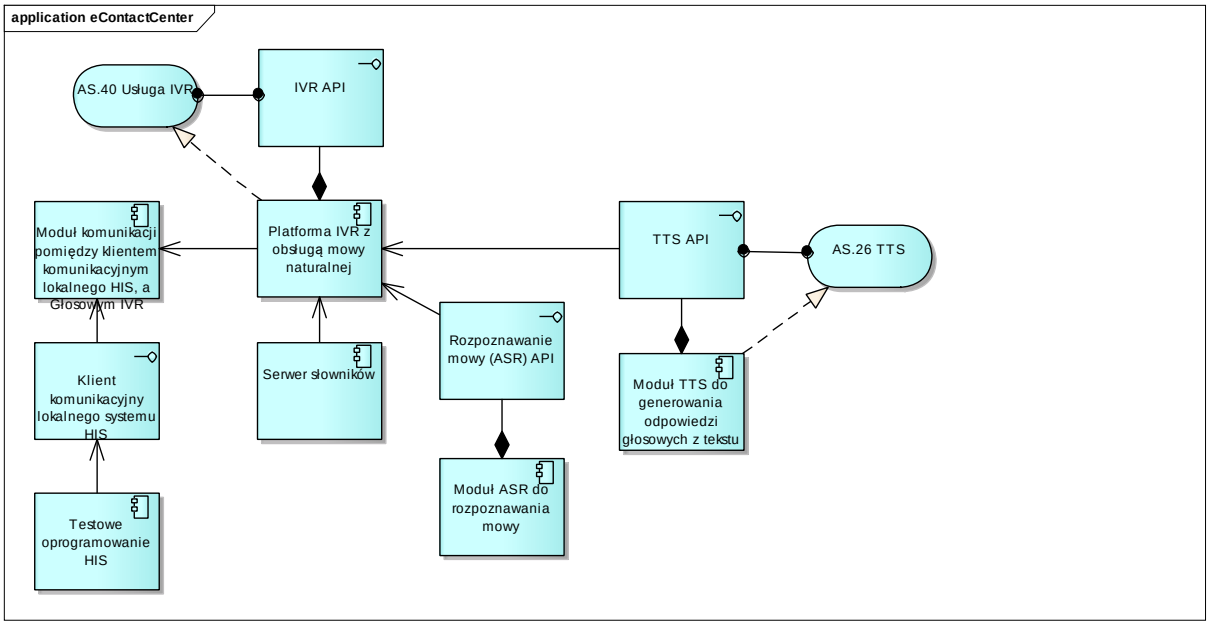
| ID wymagania | Opis wymagania |
|---|---|
| TTS.1. | Usługa TTS musi umożliwiać zamianę tekstu komputerowego (ciąg znaków) na mowę w trakcie połączenia telefonicznego. |
| TTS.2. | Usługa TTS musi pozwalać na generowanie mowy w języku polskim (informacje zgromadzone w bazie muszą być odczytywane w języku polskim). |
| TTS.3. | Usługa TTS musi umożliwiać generowanie mowy jednocześnie dla 10 równoległych połączeń telefonicznych. |
| TTS.4. | Usługa TTS musi zapewniać generowanie pojedynczych zdań w czasie nie dłuższym niż 1 s. |
| TTS.5. | Usługa TTS musi zapewniać możliwość rozszerzenia funkcjonalności o dodatkowe języki naturalne. |
| TTS.6. | Usługa TTS musi wykorzystywać słowniki zawarte w usłudze słownikowej. |

## 4.5 IVR

Usługa polega na udostępnianiu w sposób automatyczny za pośrednictwem głosowego połączenia telefonicznego informacji dotyczących funkcjonowania placówki medycznej, które będą definiowane na etapie wykorzystania usługi IVR przez twórców aplikacji.

Dodatkowo jako usługa musi być dostępny mechanizm rejestracji na wizytę przy użyciu głosowego połączenia telefonicznego.

Informacje te i usługi muszą być udostępnione w sposób automatyczny za pośrednictwem głosowego połączenia telefonicznego. System komputerowy świadczący te usługi będzie wykorzystywał technologie rozpoznawania mowy, przetwarzania mowy naturalnej (analizy semantycznej) oraz generowania odpowiedzi mówionej.




Rysunek 9 Usługa IVR

Minimalne wymagania dla usługi IVR:

| ID wymagania | Opis wymagania |
|---|---|
| IVR.1. | Usługa musi składać się co najmniej z następujących modułów funkcjonalnych:<br>• klient komunikacyjny lokalnego systemu HIS<br>• moduł komunikacji pomiędzy klientem komunikacyjnym lokalnego HIS a głosowym IVR<br>• moduł głosowy IVR z obsługą mowy naturalnej<br>• moduł ASR do rozpoznawania mowy |
| IVR.2. | Usługa musi mieć możliwość integracji z lokalnym systemem HIS za pomocą klienta komunikacyjnego. |
| IVR.3. | Moduł ASR (od ang. Automatic Speech Recognition – Automatyczne Rozpoznawanie Mowy), którego celem jest zamiana wypowiedzi telefonicznych klientów systemu na teksty komputerowe (ciąg znaków) z podaniem prawdopodobieństwa, jakie przypisane zostało każdemu rozpoznanemu słowu bądź wyrażeniu. |
| IVR.4. | Moduł rozpoznawania mowy musi działać w języku polskim z możliwością rozszerzenia o inne wersje językowe. |
| IVR.5. | Moduł ASR musi umożliwiać rozpoznawanie kilku (min. 3) kategorii informacji w jednej wypowiedzi (zdaniu), w której poszczególne kategorie występują w różnych miejscach wypowiedzi i poprzedzielane są słowami nieznaczącymi (spoza istotnych kategorii informacji) np. „podaj mi na jutro wieczór szpitale w których jest dyżur okulistyczny” |
| IVR.6. | Moduł ASR musi umożliwiać rozpoznawanie jednoczesne dla co najmniej 30 równoległych połączeń telefonicznych. |
| IVR.7. | Moduł ASR musi przekazywać do aplikacji IVR informację o prawdopodobieństwie z jakim zostały rozpoznane poszczególne części wypowiedzi. |
| IVR.8. | Usługa musi być zintegrowana z usługą TTS w zakresie generowanie mowy w języku polskim (informacje zgromadzone w bazie muszą być odczytywane w języku polskim). |
| IVR.9. | Zarządzanie połączeniami telefonicznymi. |
| IVR.10. | Przetwarzanie mowy naturalnej wydzwaniających się do niego użytkowników, bez konieczności instalowania dodatkowego oprogramowania po stronie dzwoniącego (np. jakiegokolwiek oprogramowania klienckiego na telefonach komórkowych). |
| IVR.11. | Obsługa dialogów z klientami w języku polskim z możliwością rozszerzenia o język dodatkowy. |

| | |
|---|---|
| IVR.12. | Przetwarzanie rozpoznanych przez moduł ASR wypowiedzi w języku naturalnym w czasie rzeczywistym w celu ich powiązania z realizowanymi przez system usługami (np. „chcę poznać listę przychodni specjalistycznych" vs „Informacja o wyniku badania") oraz jednocześnie ma rozpoznać na podstawie wypowiedzi, czy wypowiedź została wykonana w języku polskim czy innym dostępnym w aplikacji. |
| IVR.13. | Sterowanie dialogiem na podstawie zaprogramowanych scenariuszy dialogów z klientami. |
| IVR.14. | Usługa musi integrować się z usługą zarządzania słownikami w zakresie wykorzystania słowników terminologii medycznej. |
| IVR.15. | Usługa musi komunikować się z użytkownikiem z wykorzystaniem publicznych kanałów telefonicznych oraz telefonii IP. |
| IVR.16. | Usługa musi działać w oparciu o algorytmy rozpoznawania mowy i analizy semantycznej wypowiedzi. |
| IVR.17. | Moduł komunikacyjny musi posiadać funkcje autosprawdzania celem potwierdzenia poprawności komunikacji i sprawności klienta komunikacyjnego |
| IVR.18. | Usługa musi generować odpowiedź dla użytkownika w czasie rzeczywistym z wykorzystaniem mechanizmów syntezy mowy |
| IVR.19. | Usługa musi zawierać bazę ontologiczną języka polskiego wraz z systemem obliczania odległości semantycznej dwóch wypowiedzi wygłoszonych w języku naturalnym w czasie nie przekraczającym 0,1 sekundy |
| IVR.20. | Usługa musi umożliwiać rejestrowanie połączeń przychodzących. |
| IVR.21. | Usługa musi zawierać kompletny zestaw narzędzi do tworzenia dialogów (szablonów/schematów) w języku naturalnym. |
| IVR.22. | Usługa musi umożliwiać przetwarzanie zapytań w oparciu o dane przechowywane w lokalnej lub zewnętrznej bazie danych. |
| IVR.23. | Usługa musi umożliwiać implementację nielimitowanej liczby gramatyk |
| IVR.24. | Usługa musi umożliwiać tworzenie gramatyk bez limitu słów |
| IVR.25. | Jeśli usługa wymaga licencji na inne niż domyślne środowisko bazodanowe to Wykonawca musi dostarczyć licencję na każdy dodatkowy silnik bazodanowy w liczbie pozwalającej na jego uruchomienie na infrastrukturze serwerowej składającej się z 2 CPU i 8 rdzeni. |

## 4.6 Obsługa apteki szpitalnej

Poniżej przedstawiono wymagania dla obsługi apteki szpitalnej.

| ID wymagania | Opis wymagania |
|---|---|
| Apt.1. | System musi umożliwiać tworzenie i zarządzanie receptariuszem szpitalnym. |
| Apt.2. | Moduł musi być dostarczany z bazą leków oraz wyposażony w narzędzie umożliwiające ich łatwe (jednym klawiszem/dwukrotnym kliknięciem myszki) przepisanie wraz ze wszystkimi niezbędnymi danymi leków do receptariusza. |
| Apt.3. | System musi umożliwiać zarządzanie receptariuszami oddziałowymi wraz z odnotowaniem statusu leku:<br>a. w receptariuszu,<br>b. dostępny do zamawiania,<br>c. dopuszczony do obrotu. |
| Apt.4. | System musi umożliwiać wykorzystanie słowników: leków, grup ATC, nazw międzynarodowych, nazw handlowych, jednostek miar, lekarzy zlecających itp. |
| Apt.5. | Zarządzanie katalogiem środków recepturowych wraz z definiowaniem jego składu. |
| Apt.6. | System musi umożliwiać definiowanie grup leków. Moduł musi pozostawiać możliwość przyporządkowania leku do wielu grup. |
| Apt.7. | System musi umożliwiać podgląd w informacje o lekach z kończącym się terminem ważności i lekach przeterminowanych. |
| Apt.8. | System musi umożliwiać konfigurację blokady obrotu lekami przeterminowanymi. |
| Apt.9. | System musi umożliwiać sporządzanie zamówień do dostawców środków farmaceutycznych i materiałów medycznych z rozbiciem na: zamówienia publiczne i zamówienia doraźne. |

| | |
|---|---|
| Apt.10. | Ilości do zamówień o których mowa w wymaganiu eHISGK.APT.9 są wyliczane automatycznie na podstawie aktualnych stanów magazynowych. |
| Apt.11. | System musi umożliwiać rejestrację (ewidencję) dostaw środków farmaceutycznych i materiałów medycznych. |
| Apt.12. | System musi umożliwiać automatyczne generowanie korekt dokumentów wewnętrznych inicjowane wprowadzeniem korekty zewnętrznej. |
| Apt.13. | System musi umożliwiać wczytanie do modułu dokumentów przychodowych (faktur), ewidencjonujących dostawy w formie elektronicznej. |
| Apt.14. | System musi umożliwiać definiowanie indywidualnych systemów kodowych dla poszczególnych dostawców. |
| Apt.15. | System musi umożliwiać rejestrację korekt do dokumentów ewidencjonujących dostawy środków farmaceutycznych i materiałów medycznych. |
| Apt.16. | System musi umożliwiać ewidencję obrotu lekami spoza receptariusza szpitalnego. |
| Apt.17. | System musi umożliwiać ewidencję zwrotów do dostawców. |
| Apt.18. | System musi umożliwiać ewidencję podpisanych umów z dostawcami wraz z aneksami. |
| Apt.19. | System musi umożliwiać weryfikację dokumentów przychodowych z podpisanymi umowami z dostawcą (kontrola cen, stopnia realizacji umowy). |
| Apt.20. | System musi umożliwiać ewidencję dostaw spirytusu i narkotyków. |
| Apt.21. | System musi umożliwiać ewidencję dostaw darów. |
| Apt.22. | System musi umożliwiać ewidencję dostaw towarów nie stanowiących własności szpitala (oddanych w komis). |
| Apt.23. | System musi umożliwiać ewidencję indywidualnego importu docelowego. |
| Apt.24. | System musi umożliwiać ewidencję przyjęcia środka pacjenta. |
| Apt.25. | System musi umożliwiać ewidencję wydania do jednostki zewnętrznej. |
| Apt.26. | System musi umożliwiać przyjmowanie zamówień z jednostek organizacyjnych:<br>a. ręczne,<br>b. elektroniczne. |
| Apt.27. | System musi umożliwiać ewidencję zwrotów z oddziałów:<br>a. ręczne,<br>b. elektroniczne. |
| Apt.28. | System musi umożliwiać automatyczną realizacji zamówień przychodzących z apteczek oddziałowych i innych jednostek organizacyjnych. |
| Apt.29. | System musi zapewniać w trakcie realizacji zapotrzebowań bieżące informacje o:<br>a. Ilości zamówionej,<br>b. Ilości na stanie magazynowym apteki,<br>c. Ilości w drodze,<br>d. Ilości na stanie apteczki oddziałowej. |
| Apt.30. | System musi umożliwiać cofnięcie wydania do jednostki organizacyjnej. |
| Apt.31. | System musi umożliwiać ewidencję sporządzania leków recepturowych z wykorzystaniem automatycznego mechanizmu doboru składników z wcześniej wprowadzonego składu receptury lub poprzez ręczne zdejmowanie składników receptury. W składzie receptury istnieje możliwość wykorzystania zamienników składników recepturowych. |
| Apt.32. | System musi umożliwiać ewidencję sporządzania: preparatów laboratoryjnych, preparatów galenowych oraz płynów infuzyjnych z wykorzystaniem mechanizmów sporządzania leków recepturowych. |
| Apt.33. | System musi umożliwiać ewidencję sporządzania roztworów spirytusowych. |
| Apt.34. | System musi umożliwiać zaznaczenie pozycji receptariusza do późniejszego wykorzystania w różnych miejscach aplikacji (np. przy tworzeniu zamówień do dostawców). |
| Apt.35. | System musi umożliwiać ewidencję ubytków i strat nadzwyczajnych. |
| Apt.36. | System musi umożliwiać generowanie i drukowanie arkusza do spisu z natury. |
| Apt.37. | System musi umożliwiać korektę stanów magazynowych (ilościowa i jakościowa) na podstawie arkuszy spisu z natury. |
| Apt.38. | System musi umożliwiać wykonywania zestawień dla poszczególnych grup. |
| Apt.39. | System musi pozwalać na generowanie bieżących raportów i zestawień umożliwiających m.in.: |

| | |
|---|---|
| | a. przegląd stanów magazynowych na wybrany dzień,<br>b. przegląd bieżących stanów magazynowych,<br>c. analizę zużycia środków farmakologicznych,<br>d. analizę obrotów środków farmakologicznych. |
| Apt.40. | System musi pozwalać na generowanie bieżących raportów i zestawień umożliwiających analizę przychodów i rozchodów m.in. według:<br>a. środków,<br>b. dostawców, jednostek organizacyjnych,<br>c. pacjentów,<br>d. dokumentów,<br>e. klasyfikacji ATC. |
| Apt.41. | System musi pozwalać na generowanie bieżących raportów i zestawień umożliwiających m.in.:<br>a. kontrolę leków o zbliżającym się terminie końca daty ważności,<br>b. rozliczenie i kontrolę odbiorców leków,<br>c. rozliczenie i kontrolę dostawców leków, włącznie z rozliczeniem zamówień publicznych,<br>d. indywidualne rozliczenie pacjentów,<br>e. drukowanie księgi przychodów i rozchodów narkotyków i leków psychotropowych |
| Apt.42. | System musi udostępniać Generator raportów definiowanych przez użytkownika. |
| Apt.43. | System musi pozwalać na obsługę wielu magazynów. |
| Apt.44. | System musi pozwalać na zdefiniowanie odrębnego magazynu komisu, na którym przechowywane będą towary nie stanowiące własności szpitala (oddane w komis) |
| Apt.45. | System musi pozwalać na przegląd aktualnych stanów magazynowych z możliwością wglądu w: informacje o leku, obroty i dostawy dla każdego leku lub materiału:<br>a. z wybranego magazynu,<br>b. z wybranego miejsca składowania,<br>c. wybranej grupy leków. |
| Apt.46. | System musi pozwalać na definiowane receptariuszy oddziałowych. |
| Apt.47. | System musi pozwalać na przegląd i kontrolę stanów magazynowych oraz obrotów w magazynach apteczek oddziałowych. |
| Apt.48. | System musi pozwalać na wspomaganie przygotowywania przetargów publicznych w zakresie określenia listy leków i materiałów, ich ilości (wyliczanych na podstawie dotychczasowego zużycia ) oraz szacowanej wartości. |
| Apt.49. | System musi pozwalać na kontrolę i monitorowanie realizacji przetargu. |
| Apt.50. | System musi pozwalać na obsługę danych archiwalnych. |
| Apt.51. | System musi pozwalać na komunikację z aplikacjami wchodzącymi w skład ERP w zakresie przekazywania faktur, dokumentów kosztowych. |
| Apt.52. | System musi pozwalać na komunikację z modułem Ruch Chorych w zakresie aktualizacji stanu Apteczki Oddziałowej, zgodnie z ewidencją dystrybucji środków farmaceutycznych odnotowywanych w Ruchu Chorych. |
| Apt.53. | System musi pozwalać na współpracę z czytnikami kodów kreskowych i kolektorami danych w zakresie co najmniej identyfikacji leku, oraz generowania wydania na podstawie zeskanowanych leków. |
| Apt.54. | System musi pozwalać na obsługę komisu, w którym przechowywane będą towary nie stanowiące własności szpitala (oddane w komis) w minimalnym zakresie funkcjonalnym:<br>a. Możliwość definiowania słowników: rozmiarów asortymentów, grup elementów składowych pakietów asortymentowych, grup analitycznych pakietów asortymentowych.<br>b. Możliwość ewidencji umowy na prowadzenie komisu z minimalnym zakresem danych: okres obowiązywania, Ilości grup asortymentowych, ilość pakietów, wartość poszczególnych grup i pakietów.<br>c. Możliwość ewidencji przyjęcia towaru do komisu na podstawie:<br>i) PZ tworzonego w oparciu o WZ dostawcy,<br>ii) PZ tworzonego w oparciu o ceny z umowy (w przypadku brak WZ).<br>d. Możliwość realizacji wydania z komisu do jednostki szpitalnej na podstawie zapotrzebowania. |

| | |
|---|---|
| | e. Automatyczne generowanie do dostawcy zamówień na fakturę na podstawie zużycia na pacjenta.<br>f. Możliwość ewidencji faktur zakupu na podstawie zamówień do producenta z komisu.<br>g. Możliwość ewidencji zakupu towaru spoza umów.<br>h. Możliwość wparcia ewidencji przychodów w oparciu o kody kreskowe.<br>i. Możliwość automatycznego rozchodu przyjętego towaru z jednoczesną korektą obrotu towaru komisowego na podstawie przyjętej faktury:<br>i) z apteki do apteczki jednostki,<br>ii) zużycie towaru na pacjenta.<br>j. Możliwość analizy i wglądu w stopień realizacji umowy na komis.<br>k. Możliwość wygenerowania raportu wyłącznie ilościowego (bez wartości) z realizacji umowy w tym także do pliku.<br>l. Możliwość wygenerowania raportu ilościowo – wartościowego z realizacji umowy.<br>m. Możliwość wygenerowania raportu szczegółowego z realizacji umowy z minimalnym zakresem danych:<br>i) Pacjent,<br>ii) Jednostka organizacyjna zamawiająca towar,<br>iii) Grupa analityczna pakietu,<br>iv) Kwota,<br>v) Dostawca. |

# 5 Infrastruktura techniczna

Zakres funkcjonalny i pozafunkcjonalny usług biznesowych i aplikacyjnych stawia istotne wymagania dotyczące usług technicznych. Każda z usług biznesowych oraz wspierające ich świadczenie aplikacji biznesowych i infrastrukturalnych została wyskalowana pod kątem wymagań infrastrukturalnych. W następstwie powstał projekt infrastruktury technicznej obejmującej wymagania dotyczące:

- Infrastruktury sieciowej dla komory podstawowej
- Infrastruktury serwerowej
- Infrastruktury macierzowej
- Infrastruktury bazodanowej
- Infrastruktury programowej

Wykonawca jest zobowiązany do dostarczenia i uruchomienia wskazanej w niniejszej sekcji infrastruktury oraz uruchomienia na niej usług biznesowych oraz wspierających ich świadczenie usług aplikacyjnych.

Wszystkie wymagania dotyczą jednej, podstawowej komory.

## 5.1 Zestawienie ilościowe elementów infrastruktury technicznej

Wykonawca jest zobowiązany do dostarczenia elementów infrastruktury technicznej w liczbie wskazanej w poniższej tabeli.

Tabela 1 Zestawienie ilościowe elementów infrastruktury technicznej

| Grupa elementów | Nazwa elementu | Sekcja | Liczba | Szczegółowy termin wsparcia |
|---|---|---|---|---|
| **Infrastruktura sieciowa komory podstawowej** | Przełącznik SAN | 5.2.1 | 2 | |
| | System SIEM dla ochrony sieci | 5.2.2 | 2 | |
| **Infrastruktura serwerowa typu blade** | Infrastruktura blade | 5.3.1 | 2 | |
| | Zarządzanie infrastrukturą blade | 5.3.2 | 1 | |
| | Serwery typu blade1 | 5.3.3 | 8 | |
| | Serwery typu blade3 | 5.3.4 | 21 | |
| | Serwer zarządzający | 5.3.5 | 2 | |
| | Serwery do backupu | 5.3.6 | 1 | |
| | Szafy serwerowe | 5.3.7 | 2 | |
| **Infrastruktura macierzowa** | Półki na dyski dla macierzy operacyjnej (produkcyjnej) | 5.4.1 | 2 | |
| | Półki na dyski dla macierzy kopii zapasowych | 5.4.2 | 1 | |
| **Infrastruktura bazodanowa** | Serwer bazodanowy (DBMS) | 5.5.1 | 16 rdzeni architektury x86 | 1 rok |
| | Opcje dodatkowe | 5.5.2 | 16 rdzeni architektury x86 | 1 rok |

| | | | | |
|---|---|---|---|---|
| | System SIEM dla ochrony środowiska bazodanowego | 5.5.3 | 2 | |
| **Infrastruktura programowa** | System operacyjny klasy Linux w wersji serwerowej (Enterprise) przeznaczony do instalacji na serwerach obsługujących usługi aplikacyjne infrastrukturalne, w tym platformę integracji i budowania usług złożonych oraz usługi aplikacyjne biznesowe | --- | 25 serwerów architektury x86 max. 2 CPU | 1 rok |
| | Platforma wirtualizacyjna | 5.6.1 | 16 CPU | |
| | Serwer aplikacji | 5.6.2 | 17 CPU architektury x86 | 1 rok |
| | Infrastruktura cache | 5.6.3 | 1 CPU, 4 rdzenie architektury x86 | 1 rok |
| | Serwer www dostarczony przez tego samego producenta co serwer aplikacji | --- | 1 CPU, 4 rdzenie architektury x86 | 1 rok |
| | Oprogramowanie antywirusowe | 5.6.4 | 1 | |
| | Oprogramowanie do backupu i archiwizacji | 5.6.5 | 1 | |
| **Infrastruktura integracji i budowania usług złożonych** | Szyna usługowa | 5.7.1 | 8 rdzenie architektury x86 | 1 rok |
| | Silnik procesów biznesowych | 5.7.2 | 4 rdzenie architektury x86 | 1 rok |

## 5.2 Infrastruktura sieciowa komory podstawowej

Wykonawca musi wyposażyć we wskazany sprzęt sieciowy jedną komorę (podstawową, wskazaną przez Zamawiającego).

### 5.2.1 Przełącznik SAN

Przełącznik SAN typu FC spełniający następujące parametry:

| ID wymagania | Treść wymagania |
|---|---|
| INF.SIEC.1. | Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 10, 8, 4, 2 Gb/s. W przypadku obsadzenia portu za pomocą SFP 16Gb/s przełącznik musi zapewniać funkcję autonegocjacji prędkości 16, 8 i 4 Gb/s. W przypadku obsadzenia portu za pomocą SFP 8Gb/s przełącznik musi zapewniać funkcję autonegocjacji prędkości 8, 4 i 2 Gb/s. |
| INF.SIEC.2. | Przełącznik FC musi umożliwiać rozbudowę do minimum 256 portów w ramach pojedynczej obudowy, pracujących z prędkością 8, 4, 2 Gb/s. Przełącznik FC musi umożliwiać rozbudowę do minimum 192 porty w ramach pojedynczej obudowy, pracujących z prędkością 16, 8, 4, 2 Gb/s. Przełącznik musi posiadać ilość portów oraz kabli o odpowiednich długościach wystarczającą do podłączenia wszystkich wymaganych urządzeń i ich wszystkich portów spośród: serwerów, obudów infrastruktury blade, macierzy, przełączników brzegowych sieci SAN (w ramach połączeń ISL), bibliotek taśmowych, ewentualnych urządzeń lub połączeń ISL łączących oba ośrodki. |

| | |
|---|---|
| INF.SIEC.3. | Przełącznik FC musi posiadać nie mniej niż 96 aktywnych portów FC pracujących z prędkością 8Gb/s, wyposażonych we wkładki SFP 8Gb/s. |
| INF.SIEC.4. | Przełącznik FC musi umożliwiać rozbudowę do takiej konfiguracji sprzętowej, w której 256 portów może jednocześnie pracować z pełną przepustowością min. 8Gb/s. Przełącznik FC musi umożliwiać rozbudowę do takiej konfigurację sprzętowej, w której 192 porty mogą jednocześnie pracować z pełną przepustowością min. 16Gb/s. |
| INF.SIEC.5. | Przepustowość między pojedynczą kartą z portami przełącznika FC, a „backplanem" musi wynosić, co najmniej 512 Gb/s w jednym kierunku (half duplex). |
| INF.SIEC.6. | Wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika musi być nie większa niż 2,4µs. |
| INF.SIEC.7. | Przełącznik musi obsługiwać porty: E, D, F oraz FL. |
| INF.SIEC.8. | Przełącznik FC musi umożliwiać połączenie z co najmniej 3 innymi przełącznikami FC za pomocą dedykowanych połączeń optycznych, których użycie nie może zmniejszyć maksymalnej dostępnej liczby portów służących do podłączania urządzeń końcowych takich jak serwery i macierze. Całkowita przepustowość dostępna w ramach jednej obudowy przeznaczona dla dedykowanych połączeń optycznych musi wynosić, co najmniej 1024 Gb/s w jednym kierunku (half duplex). Przełącznik musi współpracować w sposób natywny z pozostałymi przełącznikami sieci SAN, które będą przełącznikami brzegowymi zainstalowanymi w innych miejscach infrastruktury np. przełącznikami zainstalowanymi w infrastrukturze blade. |
| INF.SIEC.9. | Maksymalny pobór prądu przełącznika FC wyposażonego w 256 portów FC 8Gb/s lub 192 porty FC 16Gb/s musi być nie większy niż 1200W. |
| INF.SIEC.10. | Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 256 portów FC 8Gb/s lub 192 porty FC 16Gb/s musi być nie większa niż 4100 BTU na godzinę. |
| INF.SIEC.11. | Przełącznik FC musi być zbudowany w architekturze modularnej, umożliwiającej wymianę wszystkich modułów w czasie pracy. Musi mieć nadmiarowe zasilacze, wentylatory, płyty z procesorami sterującymi. W odniesieniu do kart portów FC, kart rozszerzeń, płyt z procesorami sterującymi, modułów portów Fibre Channel (SFP), zasilaczy i chłodzenia musi istnieć możliwość wymiany w trybie „na gorąco". W przełączniku FC czas wymiany dowolnego uszkodzonego elementu takiego jak karty FC, karty rozszerzeń, karty procesorów sterujących, karty centralnego przełączania, moduły wentylatorów, moduły zasilaczy nie może być ograniczony żadnym limitem. W przełączniku FC tzw. backplane obudowy, zapewniający połączenie pomiędzy kartami rozszerzającymi z portami FC a kartami z procesorami sterującymi i centralnego przełączania, nie może zawierać żadnych elementów aktywnych (w tym rezystorów, kondensatorów czy układów IC). |
| INF.SIEC.12. | Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Przełącznik FC musi wspierać mechanizm balansowania ruchu pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o OXID. Połączenik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o OXID. Jednoczesne wykorzystanie obu mechanizmów powinno zapewnić dla dowolnej pary komunikujących się urządzeń końcowych uzyskanie kanału komunikacyjnego o zaagregowanej przepustowości 2048Gb/s half duplex. |
| INF.SIEC.13. | Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. ASIC) na podstawie portów i adresów WWN. |
| INF.SIEC.14. | Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. |
| INF.SIEC.15. | Przełącznik FC musi wspierać mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 16 portach przełącznika FC w przypadku, gdy przełącznik wyposażony jest w odpowiednią liczbę kart rozszerzających z portami FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów. |
| INF.SIEC.16. | Przełącznik FC musi wspierać uwierzytelnianie (autentykacja) przełączników w sieci Fabric za |

| | |
|---|---|
| | pomocą protokołów DH-CHAP i FCAP. |
| INF.SIEC.17. | Przełącznik FC musi wspierać uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP. |
| INF.SIEC.18. | Przełącznik FC musi wspierać szyfrowanie połączenia z konsolą administracyjną. |
| INF.SIEC.19. | Przełącznik FC musi wspierać protokół SSHv2. |
| INF.SIEC.20. | Przełącznik FC musi wspierać definiowane kont użytkowników w środowisku sieci SAN opartych o usługi katalogowe dostarczone w ramach zamówienia. |
| INF.SIEC.21. | Przełącznik FC musi wspierać szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS. |
| INF.SIEC.22. | Przełącznik FC musi wspierać obsługę SNMP v3. |
| INF.SIEC.23. | Przełącznik FC musi mieć możliwość wykonania pełnej konfiguracji przez: komendy tekstowe w interfejsie znakowym oraz przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. |
| INF.SIEC.24. | Przełącznik FC musi być wyposażony w narzędzia do logowania zdarzeń poprzez mechanizm „syslog”. |
| INF.SIEC.25. | Przełącznik FC musi być wyposażony w narzędzia do monitoringu wydajności end-to-end umożliwiających pomiar przepustowości między wybranymi parami komunikujących się urządzeń. |
| INF.SIEC.26. | Przełącznik FC musi być wyposażony w narzędzia do monitorowania połączeń fizycznych i połączeń typu „trunk”. |
| INF.SIEC.27. | Przełącznik FC musi być wyposażony w narzędzia do ciągłego monitorowanie parametrów pracy przełącznika i sieci fabric z automatycznym powiadamianiem administratora w przypadku przekroczenia wartości granicznych. |
| INF.SIEC.28. | Przełącznik FC musi być wyposażony w narzędzia do identyfikowanie urządzeń końcowych, które zbyt wolno przetwarzają dane i spowalniają inne przepływy danych współdzielące te same połączenia ISL wywołując tym samym problemy wydajnościowe w sieci fabric. |
| INF.SIEC.29. | Przełącznik FC musi być wyposażony w narzędzia do jednoznacznej identyfikacji do jakiego przepływu danych (identyfikacja na bazie SID, DID oraz FID) przynależały odrzucone ramki (discarded frames) z możliwością wyświetlenia zawartości ich pierwszych 64 bajtów. |
| INF.SIEC.30. | Przełącznik FC musi być wyposażony w narzędzia dające możliwość skonfigurowania specjalnego portu diagnostycznego tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających sprawność połączeń elektrycznych z modułem SFP, połączenia optycznego między dwoma przełącznikami oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla SFP 16Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric. |
| INF.SIEC.31. | Przełącznik FC musi być wyposażony w oprogramowanie zarządzające pozwalające na wykrywanie i wizualizację topologii infrastruktury (graficzny schemat połączeń i zależności pomiędzy przełącznikami FC i innymi elementami sieci SAN takimi jak wirtualne maszyny, serwery, macierze, karty HBA). |
| INF.SIEC.32. | Przełącznik FC musi być wyposażony w narzędzia do analizy utylizacji zasobów, ułatwiające planowanie przyszłych zmian środowiska pamięci masowych na podstawie danych bieżących, jak i historycznych (tzw. Capacity Planing). |
| INF.SIEC.33. | Przełącznik FC musi być wyposażony w narzędzia do tworzenia różnego rodzaju raportów na potrzeby procesu Capacity Planing. |
| INF.SIEC.34. | Przełącznik FC musi być wyposażony w narzędzia do korelacji zdarzeń pochodzących z przełącznika ze zdarzeniami pochodzącymi z innych elementów sieci SAN (macierze, serwery, maszyny wirtualne, aplikacje). |
| INF.SIEC.35. | Przełącznik FC musi być wyposażony w narzędzia do definiowania i wysyłania powiadomień do administratora lub uruchomienie skryptu. |
| INF.SIEC.36. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric, które musi być wyposażone w graficzny interfejs użytkownika, pozwalające na włączanie i wyłączanie portów (i całych przełączników) w wielu urządzeniach jednocześnie. |
| INF.SIEC.37. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym |

| | |
|---|---|
| | klasy Director) w wielu sieciach fabric pozwalające na wyświetlanie stanu poszczególnych portów i modułów. |
| INF.SIEC.38. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric pozwalające na wizualizację fizycznych połączeń miedzy urządzeniami z podaniem informacji (stan, prędkość, typ) o łączach między nimi. |
| INF.SIEC.39. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric pozwalające na wizualizację statystyk poszczególnych portów i modułów. |
| INF.SIEC.40. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric pozwalające na gromadzenie i wizualizację historycznych danych o wydajności sieci na poziomie pojedynczego portu. |
| INF.SIEC.41. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric pozwalające na utworzenie i przechowywanie repozytorium wersji firmware'u. |
| INF.SIEC.42. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric pozwalające na wgrywanie aktualizacji firmware'u do wielu przełączników jednocześnie inicjowane z pojedynczej konsoli zarządzającej. |
| INF.SIEC.43. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric posiadające wbudowane narzędzie wspomagania operacji łączenia dwóch sieci fabric (narzędzie musi porównywać parametry FC, bazy zoningu etc. i wskazywać wszystkie niezgodności uniemożliwiające połączenie obu sieci w jeden fabric). |
| INF.SIEC.44. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric posiadające narzędzie do zarządzania zmianą umożliwiające monitorowanie zmian zachodzących w sieci oraz późniejsze ich porównywanie na podstawie raportów. |
| INF.SIEC.45. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric posiadające możliwość automatycznego przesyłania informacji do serwisu w przypadku wystąpienia problemów z przełącznikami tzw. ""call home"". Funkcja musi obsługiwać komunikację za pomocą modemu lub poprzez sieć Internet jak i umożliwiać przesyłanie wiadomości email. |
| INF.SIEC.46. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric posiadające narzędzie do zarządzania zoningiem oraz umożliwiające przechowywanie w bazie danych wielu różnych konfiguracji zoningu oraz ich edycję w trybie offline. |
| INF.SIEC.47. | Wymagane jest oprogramowanie do konfiguracji i monitorowania wielu przełączników (w tym klasy Director) w wielu sieciach fabric posiadające konfigurowanie sekwencyjnych, planowych rebootów całych grup przełączników. |
| INF.SIEC.48. | Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. |
| INF.SIEC.49. | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, szeregowy oraz inband IP-over-FC. |
| INF.SIEC.50. | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |
| INF.SIEC.51. | W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisania co najmniej jednego dedykowanego administratora. Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą dedykowanych połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric. |
| INF.SIEC.52. | Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu na podstawie adresów WWW komunikujących się urządzeń. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości |

| | |
|---|---|
| | parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie. Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi być możliwość określenia wartości limitu przepustowości danych wchodzących niższej niż wynegocjowana prędkość portu. |
| INF.SIEC.53. | W przełączniku musi istnieć możliwość instalacji kart rozszerzających jego funkcjonalność o obsługę protokołu FCIP za pomocą portów 10GbE. W przełączniku musi istnieć możliwość instalacji kart rozszerzających jego funkcjonalność o możliwość szyfrowania danych na macierzach dyskowych i napędach taśmowych. Przepustowość szyfrowania danych dostępna w ramach pojedynczej karty szyfrującej nie może być mniejsza niż 48Gb/s. |
| INF.SIEC.54. | Przełącznik musi posiadać wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |

### 5.2.2 System SIEM dla ochrony sieci

Infrastruktura (sprzęt oraz oprogramowanie) klasy SIEM służące do ochrony sieci i umożliwiające świadczenie usług firewall, IPS (Intrusion Prevention System), NAT oraz IPSec.

Wymagania minimalne:

| ID wymagania | Opis wymagania |
|---|---|
| INF.FIR.1. | Firewall musi być dostarczony jako dedykowane urządzenie sieciowe w postaci chassis o wysokości do 16 U, przystosowanego do montażu w szafie rack, wymienne wentylatory oraz źródła zasilania AC. Musi istnieć możliwość wyposażenia w nadmiarowe źródło zasilania w celu zapewnienia redundancji zasilania N+1. |
| INF.FIR.2. | Firewall musi posiadać wymienne karty monitorujące status systemu (wentylatory, źródła zasilania, itp.), karty z interfejsami sieciowymi oraz karty usługowe realizujące funkcje bezpieczeństwa. |
| INF.FIR.3. | Zarządzanie i konfiguracja firewalla przez administratorów musi być realizowana przez moduł kontrolny. Moduł kontrolny musi sterować i monitorować pracę komponentów firewalla. Ruch tranzytowy użytkowników przechodzący przez firewall nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi być wyposażony w co najmniej 2 GB pamięci RAM, dysk twardy, oraz interfejs Ethernet służący do zarządzania. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. |
| INF.FIR.4. | System operacyjny firewalla musi śledzić stan sesji użytkowników (*stateful processing*), tworzyć i zarządzać tablicą stanu sesji. |
| INF.FIR.5. | Firewall musi obsługiwać karty z interfejsami sieciowymi, które posiadają nie mniej niż 4 porty 10 Gigabit Ethernet XFP lub SFP+ oraz karty, które posiadają nie mniej niż 7 portów Gigabit Ethernet SFP. Firewall musi posiadać 2 sloty, które mogą obsługiwać karty z interfejsami sieciowymi. Firewall musi być dostarczony z 4 interfejsami 10 Gigabit Ethernet SFP+/XFP wyposażonymi w odpowiednie moduły obsługujące standard 10GbE SR. |
| INF.FIR.6. | Realizacja mechanizmów bezpieczeństwa musi się odbywać na wyspecjalizowanych kartach usługowych posiadających własne procesory oraz wyposażonych w nie mniej 8 GB pamięci RAM. Wszystkie karty usługowe muszą posiadać identyczną funkcjonalność i pracować pod kontrolą systemu operacyjnego firewalla – nie dopuszcza się możliwości realizacji całości lub części ww. funkcji bezpieczeństwa przez karty działające pod kontrolą innych systemów operacyjnych. Zwiększenie wydajności ww. funkcji bezpieczeństwa musi się odbywać przez zwiększanie ilości kart usługowych. Firewall musi posiadać co najmniej 11 slotów pozwalających na zainstalowanie i uruchomienie kart serwisowych. Nie dopuszcza się również sytuacji, aby poszczególne moduły serwisowe były traktowane przez system operacyjny firewalla jako niezależne urządzenia, z osobnymi regułami polityki firewall – z punktu widzenia systemu operacyjnego firewalla wszystkie moduły usługowe muszą być integralną częścią urządzenia i |

| | |
|---|---|
| | wszystkie muszą podlegać tej samej polityce bezpieczeństwa konfigurowanej na module kontrolnym. |
| INF.FIR.7. | Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji z wydajnością nie mniejszą niż 25 Gb/s. Firewall musi obsłużyć nie mniej niż 12 milionów równoległych sesji oraz zestawić nie mniej niż 240 tysięcy nowych połączeń/sekundę. Jednocześnie musi istnieć możliwość rozbudowy urządzenia by obsługiwało dla funkcji Stateful Firewall odpowiednio co najmniej przepustowość 200 Gb/s, 60 milionów równoległych sesji oraz 330 tysięcy nowych sesji/sekundę. |
| INF.FIR.8. | Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. |
| INF.FIR.9. | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. |
| INF.FIR.10. | Firewall musi identyfikować aplikacje bez względu na numery portów oraz wybrane protokoły tunelowania i szyfrowania (włącznie z aplikacjami typu Peer-to-Peer i Instant Messaging). |
| INF.FIR.11. | Firewall musi mieć możliwość identyfikacji nie mniej niż 900 różnych aplikacji, w szczególności takich, które są tunelowane w protokołach HTTP i HTTPS – nie mniej niż Skype, Gadu-Gadu, Facebook, Youtube. Dostęp użytkowników do poszczególnych aplikacji musi być konfigurowany przy pomocy reguł filtrowania uwzględniających co najmniej adresy IP oraz wyżej wymienione aplikacje. Kontrola dostępu do dynamicznie identyfikowanych aplikacji musi być wykonywana z przepustowością nie mniej niż 7 Gb/s. Firewall musi umożliwiać rozbudowę w celu wykonywania kontroli dynamicznie identyfikowanych aplikacji z wydajnością co najmniej 110 Gb/s. Nie wymaga się dostarczenia licencji na tę funkcjonalność. |
| INF.FIR.12. | Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, *intrusion prevention*) realizowaną na modułach usługowych. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 7 Gb/s i umożliwiać rozbudowę do obsługi przepustowości IPS co najmniej 100 Gb/s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta. |
| INF.FIR.13. | Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 250 wirtualnych ruterów. |
| INF.FIR.14. | Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – obcinanie ruchu. Polityka QoS powinna być tworzona na podstawie: adresów IP, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać zaimplementowany mechanizm WRED, WFRED lub równoważny w celu przeciwdziałania występowaniu przeciążeń ruchu. |
| INF.FIR.15. | Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją tablicy stanu sesji. Przełączenie pomiędzy systemami firewall w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń. Zamawiający dopuszcza zaistnienie konieczności zakupu dodatkowych komponentów sprzętowych w celu zapewnienia redundancji połączeń między węzłami klastra.. |
| INF.FIR.16. | Zarządzanie urządzeniem musi odbywać się za pomocą wiersza linii poleceń (CLI). Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. |
| INF.FIR.17. | Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. Musi istnieć możliwość przechowywania nie mniej niż 40 poprzednich, kompletnych konfiguracji na urządzeniu lub w systemie zarządzania |

### 5.2.3 Wdrożenie i konfiguracja

Wykonawca musi dostarczyć, wdrożyć oraz dokonać konfiguracji elementów infrastruktury sieciowej, w tym przeprowadzić następujące czynności:

| ID wymagania | Treść wymagania |
|---|---|
| INF.SIEC.55. | Zaproponować logiczną strukturę sieci komputerowej opartą o protokół dynamicznego konfigurowania węzłów (DHCP) oraz przypisywanie adresu IP na podstawie adresu sprzętowego (MAC) karty sieciowej komputera. |
| INF.SIEC.56. | Montaż i podłączenie urządzeń sieciowych w szafach serwerowych |
| INF.SIEC.57. | Wykonanie fizycznych połączeń w obszarze LAN (pomiędzy przełącznikami, a szafami dystrybucyjnymi). |
| INF.SIEC.58. | Wykonanie fizycznych połączeń w obszarze SAN (pomiędzy serwerami, macierzami i biblioteką taśmową, a przełącznikami FC), w sposób redundantny i zapewniający komunikację w przypadku awarii pojedynczego połączenia. |
| INF.SIEC.59. | Wykonanie fizycznych połączeń pomiędzy obszarami LAN, SAN oraz serwerami, w sposób redundantny i zapewniający komunikację w przypadku awarii pojedynczego połączenia. |
| INF.SIEC.60. | Wykonanie fizycznych połączeń urządzeń sieci bezprzewodowej do portów PoE przełączników sieciowych. |
| INF.SIEC.61. | Montaż i podłączenie routerów posiadanych przez Zamawiającego |
| INF.SIEC.62. | Montaż i podłączenie przełączników rdzeniowych posiadanych przez Zamawiającego |
| INF.SIEC.63. | Montaż i podłączenie przełączników dostępowych posiadanych przez Zamawiającego |
| INF.SIEC.64. | Montaż i podłączenie urządzeń sieci bezprzewodowej posiadanych przez Zamawiającego |
| INF.SIEC.65. | Montaż i podłączenie urządzeń telefonii IP posiadanych przez Zamawiającego |
| INF.SIEC.66. | Montaż i podłączenie urządzeń równoważących obciążenie posiadanych przez Zamawiającego |

W zakresie konfiguracji sieci SAN:

| | |
|---|---|
| INF.SIEC.67. | Utworzenie zon na przełącznikach (pełna wzajemna izolacja portów macierzy dyskowych oraz biblioteki taśmowej jak również pełna izolacja portów „inicjatorów") w sposób zapewniający redundantny dostęp do zasobów macierzy dyskowych z każdego z dostarczonych serwerów. |

W zakresie konfiguracji sieci WAN:

| | |
|---|---|
| INF.SIEC.68. | Konfiguracja routera - wykonanie konfiguracji podstawowych parametrów takich jak administracja, uwierzytelnianie, czas, dostęp zdalny. |
| INF.SIEC.69. | Konfiguracja adresacji IP. |
| INF.SIEC.70. | Konfiguracja usługi VPN , utworzenie tuneli do oddziałów - utworzenie usługi bramy VPN umożliwiającej bezpieczną komunikację opartą o protokół IPSec. |
| INF.SIEC.71. | Konfiguracja funkcjonalności HA – funkcjonalność umożliwiająca automatyczne przełączenie działania na urządzenie zapasowe po awarii urządzenia podstawowego. |
| INF.SIEC.72. | Konfiguracja list dostępowych - konfiguracja poziomów dostępu dla poszczególnych hostów i podsieci, utworzenie list blokad i list dostępu dla usług sieciowych |
| INF.SIEC.73. | Konfiguracja routerów (ustanowienie tuneli VPN umożliwiających bezpieczną komunikację opartą o protokół IPSec.). |
| INF.SIEC.74. | Konfiguracja firewalla sieciowych do 50 reguł szczegółowej inspekcji. Konfiguracja modułu IPS dla celów analizy ruchu przychodzącego z sieci Internet. |
| INF.SIEC.75. | Konfiguracja firewalli aplikacyjnych (posiadanych przez Zamawiającego) |
| INF.SIEC.76. | Konfiguracja firewalli bazodanowych |

W zakresie konfiguracji sieci LAN:

| | |
|---|---|
| INF.SIEC.77. | Konfiguracja przełączników - wykonanie konfiguracji podstawowych parametrów takich jak: administracja, uwierzytelnianie, czas, dostęp zdalny. |
| INF.SIEC.78. | Utworzenie podsieci VLAN - konfiguracja przełączników do obsługi podsieci, przypisanie portów przełącznika do poszczególnych podsieci, konfiguracja routingu pomiędzy podsieciami. |
| INF.SIEC.79. | Konfiguracja Spanning Tree Protocol. |

| | |
|---|---|
| INF.SIEC.80. | Konfiguracja interfejsów L3 dla poszczególnych sieci VLAN. |
| INF.SIEC.81. | Konfiguracja rutingu pomiędzy sieciami VLAN. |
| INF.SIEC.82. | Konfiguracja połączeń pomiędzy przełącznikami oraz serwerami – konfiguracja połączeń zapewniających redundancje oraz wysoka przepustowość w obrębie szkieletu sieci. |
| INF.SIEC.83. | Zapewnienie redundancji połączeń - wykonanie konfiguracji sieci w taki sposób, aby zapewniała komunikacje pomiędzy węzłami sieci w razie awarii pojedynczego polaczenia. |
| INF.SIEC.84. | Konfiguracja uwierzytelniania 802.1X na portach dostępowych w oparciu o istniejącą instancję serwera uwierzytelniania dostarczonego w ramach zadania |

W zakresie konfiguracji sieci WIFI:

| | |
|---|---|
| INF.SIEC.85. | Konfiguracja sieci bezprzewodowej (SSID, kontrola dostępu, zabezpieczenia). |

W zakresie konfiguracji telefonii IP:

| | |
|---|---|
| INF.SIEC.86. | Konfiguracja i uruchomienie telefonii IP w lokalizacji wskazanej przez Zamawiającego. |

## 5.3 Infrastruktura serwerowa typu blade

Wykonawca musi dostarczyć i uruchomić serwery typu blade spełniające poniższe parametry.

### 5.3.1 Infrastruktura blade

Wymagania w zakresie infrastruktury blade:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BLA.1. | Infrastruktura musi być przystosowana do montażu w szafie typu rack 19”, umożliwiająca obsadzenie wszystkich wymaganych serwerów bez konieczności rozbudowy o kolejne elementy sprzętowe. |
| INF.BLA.2. | W ramach infrastruktury (pojedynczego zestawu), należy dostarczyć ilość obudów zapewniających powyższe możliwości rozbudowy, każda obudowa wchodząca w skład infrastruktury musi posiadać identyczną konfigurację (w szczególności tę samą konfigurację wyprowadzeń LAN oraz SAN). Pojedyncza obudowa musi umożliwiać montaż minimum 16 serwerów dwuprocesorowych opisanych wymaganiami, wysokość pojedynczej obudowy nie może przekraczać 10U. |
| INF.BLA.3. | Możliwość umieszczania w ramach pojedynczej obudowy wszystkich modeli serwerów blade danego producenta dostępnych w aktualnej ofercie handlowej. |
| INF.BLA.4. | Każda obudowa wchodząca w skład infrastruktury dla serwerów blade musi posiadać minimum 2 moduły typu 10Gb Ethernet wyprowadzające sygnały z minimum 2 portów sieciowych 10Gb na serwerach. Urządzenia te muszą umożliwiać agregację połączeń LAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów LAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł powinien posiadać minimum 8 portów 10Gb przygotowanych do obsadzenia modułami SFP+. Wraz z modułami należy dostarczyć minimum 16 moduły SFP+ 10Gb (po 8 na moduł) |
| INF.BLA.5. | Każda obudowa wchodząca w skład infrastruktury dla serwerów blade musi posiadać minimum dwa moduły typu 8Gb Fibre-Channel wyprowadzające sygnały z minimum 2 portów FC na serwerach ( po jednym porcie serwera na moduł). Urządzenia te muszą umożliwiać agregację połączeń SAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów SAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł musi posiadać minimum 8 zewnętrznych portów. Wszystkie porty muszą być aktywne. Wraz z modułami należy dostarczyć minimum 8 modułów SFP+ 8Gb (po 4 sztuk na moduł). |
| INF.BLA.6. | Zastosowane w ramach każdej obudowy wchodzącej w skład infrastruktury dla serwerów blade moduły LAN i SAN muszą mieć funkcjonalność przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania blade dla poszczególnych wnęk na serwery w obudowie. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet i Fibre-Channel na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta może być |

| | |
|---|---|
| | realizowana zarówno poprzez moduły LAN i SAN w infrastrukturze jak i poprzez dodatkowe oprogramowanie producenta serwerów blade. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak aby między wydzielonymi sieciami nie było komunikacji. Wymagana jest możliwość boot'owania systemów operacyjnych zainstalowanych na poszczególnych serwerach blade bezpośrednio z macierzy w środowisku SAN. Wymagane wszystkie niezbędne licencje na opisaną funkcjonalność dla całej infrastruktury blade.W przypadku sieci LAN, musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 100Mb/s do 10Gb/s. |
| INF.BLA.7. | Po zainstalowaniu wszystkich wymaganych modułów komunikacyjnych w pojedynczej obudowie wchodzącej w skład infrastruktury blade muszą być co najmniej 2 miejsca nieobsadzone, pozwalające na instalację dodatkowych modułów komunikacyjnych. |
| INF.BLA.8. | Każda z obudów na serwery wyposażona w zestaw redundantnych wiatraków (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory muszą być niezależne od zasilaczy, wymiana. Wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza (zasilaczy). |
| INF.BLA.9. | Każda z obudów wyposażona w zestaw zasilaczy redundantnych typu Hot Plug. System zasilania zdolny do obsługi awarii połowy z zainstalowanych zasilaczy (dowolne N zasilaczy przy założeniu konfiguracji N + N), wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. |
| INF.BLA.10. | Wymiana zasilacza nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów). |
| INF.BLA.11. | Każda obudowa wchodząca w skład infrastruktury dla serwerów blade musi mieć zainstalowane dwa redundantne, sprzętowe moduły zarządzające , typu Hot Plug , oraz zintegrowany w modułach zarządzających lub w obudowie, moduł KVM, umożliwiający podłączenie klawiatury, myszy i monitora |
| INF.BLA.12. | Każda z obudów wchodzących w skład infrastruktury musi posiadać identyczną konfigurację sprzętową w zakresie zasilaczy, wiatraków oraz modułów I/O |

### 5.3.2 Zarządzanie infrastrukturą blade

Wymagania w zakresie zarządzania infrastrukturą blade:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BLA.13. | Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera |
| INF.BLA.14. | Zdalne udostępnianie napędu CD-ROM/DVD/ISO na potrzeby każdego serwera z możliwością bootowania z w/w napędów. |
| INF.BLA.15. | Zdalny z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu. |
| INF.BLA.16. | W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach infrastruktury |
| INF.BLA.17. | Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego |
| INF.BLA.18. | Wymaga się aby zarządzanie całą infrastrukturą odbywało się w oparciu o jednolite oprogramowanie. Oprogramowanie musi w sposób graficzny wizualizować stan poszczególnych elementów infrastruktury (stan normalnej pracy, uwagi, awarie) a jednocześnie pozwalać na zarządzanie w sposób integralny i w oparciu o pojedynczy serwer zarządzania.<br>Oprogramowanie to musi wykorzystywać standardowe protokoły sieciowe takie jak: HTTP, SNMP, WBEM. W szczególności oprogramowanie to musi posiadać następujące funkcjonalności:<br>• Graficzne zobrazowanie stanu infrastruktury z możliwością przejścia od widoku ogólnego do widoku szczegółowego każdego z elementów infrastruktury (architektura drill-down).<br>• Możliwość kontroli wersji zainstalowanych sterowników/agentów na serwerach, możliwość przeprowadzania uaktualnień sterowników/agentów zdalnie z systemu zarządzania. |

| | |
|---|---|
| | • Możliwość zdalnej reakcji na zdarzenia w infrastrukturze np. poprzez automatyczne wykonywanie skryptów, możliwość automatycznego powiadamiania administratorów poprzez e-mail.<br>• Dostęp do aplikacji zarządzającej powinien być możliwy z serwera zarządzającego lub dowolnego innego miejsca poprzez przeglądarkę internetową (połączenie szyfrowane SSL) bez konieczności instalowania dodatkowego oprogramowania producenta serwera.<br>• Wykrywanie i przypisywanie do serwerów kart zarządzających.<br>• Możliwość monitorowania zużycia energii dla jednego lub grupy serwerów. Możliwość nakładania limitów zużycia mocy na serwer lub grupę serwerów (w ramach możliwości technologii x86-64).<br>• Możliwość uzyskania szczegółowych informacji o serwerze odnośnie jego komponentów, firmware'ow, systemu operacyjnego, adresu IP.<br>• Monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe, a także komponentów maszyn wirtualnych takich jak: wirtualny procesor, pamięć RAM dyski twarde, interfejsy sieciowe. |
| INF.BLA.19. | Licencje na powyższą funkcjonalność na wszystkie serwery blade możliwe do obsadzenia w oferowanej infrastrukturze blade. System zarządzający musi umożliwiać zarządzanie wszystkimi obudowami na serwery blade, które będą dostarczone w ramach infrastruktury dla serwerów blade. |
| INF.BLA.20. | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |

### 5.3.3 Serwery typu blade1

Wymagania dla serwera typu blade1:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BLA.21. | Obudowa typu blade, kompatybilna z oferowanymi obudowami na serwery typu blade |
| INF.BLA.22. | Procesory minimum czterordzeniowe, x86 - 64 bity, osiągające w testach SPECint_rate2006 wynik nie gorszy niż 225 punktów dla konfiguracji testowej z dwoma procesorami. Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów. |
| INF.BLA.23. | Płyta główna przygotowana do instalacji min. 2 procesorów wielordzeniowych |
| INF.BLA.24. | Minimum 1 zainstalowany procesor |
| INF.BLA.25. | Minimum 128 GB RAM DDR3 Registered DIMMs. Możliwość instalacji w serwerze minimum 512 GB pamięci RAM. Minimum 16 slotów na pamięć. |
| INF.BLA.26. | Sterownik dysków wewnętrznych: Macierzowy, RAID 0, 1. |
| INF.BLA.27. | Możliwość instalacji minimum dwóch dysków SAS/SATA/SSD typu Hot-Plug.<br>Nie wymaga się dostarczenia dysków z serwerem. Serwer musi mieć możliwość boot'owania z sieci SAN (Fibre Channel). |
| INF.BLA.28. | Minimum jeden wewnętrzny port USB. |
| INF.BLA.29. | Minimum 2 Interfejsy sieciowe 10Gb Ethernet z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej. |
| INF.BLA.30. | Minimum 2 interfejsy FC , każdy min. 8Gb |
| INF.BLA.31. | Po spełnieniu wymagań dotyczących Interfejsów sieciowych i FC, w serwerze musi pozostać minimum jeden wolny slot PCIe na dodatkową kartę rozszerzeń I/O. |
| INF.BLA.32. | Serwer wyposażony w kartę zdalnego zarządzania zapewniającą:<br>• Zdalne włączanie/wyłączanie/restart<br>• Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.<br>• Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.<br>• Podłączanie zdalnych napędów CD-ROM/DVD/ISO z możliwością bootowania z w/w napędów. |

| | |
|---|---|
| | • Podgląd logów sprzętowych serwera i karty<br>• Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). |
| INF.BLA.33. | Wspierane systemy operacyjne: Microsoft Windows 2008R2 i 2012, Oracle Linux 6, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, VMware ESXi 5. |

### 5.3.4 Serwery typu blade3

Wymagania dla serwera typu blade3:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BLA.34. | Obudowa typu blade, kompatybilna z oferowanymi obudowami na serwery typu blade |
| INF.BLA.35. | Procesory minimum ośmiordzeniowe, x86 - 64 bity, osiągający w testach SPECint_rate2006 wynik nie gorszy niż 540 punktów dla konfiguracji testowej z dwoma procesorami. Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów. |
| INF.BLA.36. | Płyta główna przygotowana do instalacji min. 2 procesorów wielordzeniowych |
| INF.BLA.37. | Liczba zainstalowanych procesorów: minimum 2 |
| INF.BLA.38. | Minimum 384 GB RAM DDR3 Registred DIMMs. Możliwość instalacji w serwerze minimum 512 GB pamięci RAM. Minimum 16 slotów na pamięć. |
| INF.BLA.39. | Sterownik dysków wewnętrznych: macierzowy, RAID 0, 1. |
| INF.BLA.40. | Możliwość instalacji minimum dwóch dysków SAS/SATA/SSD typu Hot-Plug.<br>Nie wymaga się dostarczenia dysków z serwerem. Serwer musi mieć możliwość boot'owania z sieci SAN (Fibre Channel). |
| INF.BLA.41. | Minimum jeden wewnętrzny port USB. |
| INF.BLA.42. | Minimum 2 Interfejsy sieciowe 10Gb Ethernet z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej. |
| INF.BLA.43. | Minimum 2 interfejsy FC , każdy min. 8Gb |
| INF.BLA.44. | Po spełnieniu wymagań dotyczących Interfejsów sieciowych i FC, w serwerze musi pozostać minimum jeden wolny slot PCIe na dodatkową kartę rozszerzeń I/O. |
| INF.BLA.45. | Serwer wyposażony w kartę zdalnego zarządzania zapewniającą:<br>• Zdalne włączanie/wyłączanie/restart<br>• Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.<br>• Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.<br>• Podłączanie zdalnych napędów CD-ROM/DVD/ISO z możliwością bootowania z w/w napędów.<br>• Podgląd logów sprzętowych serwera i karty<br>• Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). |
| INF.BLA.46. | Wspierane systemy operacyjne: Microsoft Windows 2008R2 i 2012, Oracle Linux 6, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, VMware ESXi 5. |

### 5.3.5 Serwer zarządzający

Wykonawca jest zobowiązany do dostarczenia serwerów przeznaczonych do oprogramowania zarządzającego i jego niezbędnych komponentów, w tym również do oprogramowania do zarządzania środowiskiem maszyn wirtualnych

Wymagania dla serwera zarządzającego typu rack:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BLA.47. | Obudowa do montażu w szafie, wysokość maksymalna 2U, wymagane dostarczenie szyn |

| | |
|---|---|
| | montażowych do szafy, wysuwanego ramienia na kable oraz wszystkich innych niezbędnych elementów potrzebnych do instalacji i poprawnego działania serwera. |
| INF.BLA.48. | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| INF.BLA.49. | Procesory minimum sześciordzeniowe, x86 - 64 bity, osiągający w testach SPECint_rate2006 wynik nie gorszy niż 435 punktów dla konfiguracji testowej z dwoma procesorami. Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów |
| INF.BLA.50. | Minimum 2 zainstalowane procesory |
| INF.BLA.51. | Minimum min. 64GB pamięci RAM RDIMM. Serwer musi być wyposażony w min 24 gniazd na moduły pamięci. Możliwość instalacji w serwerze min. 768GB RAM. Możliwość instalacji kości pamięci RDIMM lub UDIMM. |
| INF.BLA.52. | Minimum 2 sloty PCI-Express generacji 3, w tym jeden slot x16 (szybkość slotu – bus width) oraz minimum jedno gniazdo pełnej wysokości |
| INF.BLA.53. | Minimum 4 złącza typu 1GbEthernet RJ-45 |
| INF.BLA.54. | Minimum jedna karta FC zapewniająca minimum 2 interfejsy FC , każdy min. 8Gb |
| INF.BLA.55. | Wewnętrzne wnęki dyskowe przygotowane do instalacji i działania minimum ośmiu dysków SAS/SATA/SSD typu Hot-Plug . W serwerze zainstalowane min. 4 dyski twarde każdy o parametrach: 300GB , prędkość obrotowa 10000 obrotów/minutę, SAS 6G, Hot-Plug. |
| INF.BLA.56. | Dedykowany kontroler RAID min 512MB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania. Możliwe konfiguracje 0, 1, 10, 5, 50 Możliwość rozbudowy wbudowanego w płytę kontrolera dyskowego o dodatkowe funkcje, takie jak RAID 6, 60. |
| INF.BLA.57. | Serwer wyposażony w wewnętrzny napęd DVD |
| INF.BLA.58. | Minimum 4 szt. portów USB, w tym jeden wewnętrzny. |
| INF.BLA.59. | Serwer wyposażony w kartę zdalnego zarządzania zapewniającą:<br>• Zdalne włączanie/wyłączanie/restart<br>• Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.<br>• Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.<br>• Podłączanie zdalnych napędów CD-ROM/DVD/ISO z możliwością bootowania z w/w napędów.<br>• Podgląd logów sprzętowych serwera i karty<br>• Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). |
| INF.BLA.60. | Zintegrowana karta graficzna. |
| INF.BLA.61. | 2 szt. zasilaczy, redundantne, hot plug. |
| INF.BLA.62. | Chłodzenie: redundantne, hot plug. |
| INF.BLA.63. | Możliwość zainstalowania modułu TPM na płycie głównej serwera |
| INF.BLA.64. | Wspierane systemy operacyjne: Microsoft Windows 2008R2 i 2012, Oracle Linux 6, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, VMware ESXi 5. |
| INF.BLA.65. | Dostarczony system operacyjny: system operacyjny (OS ) wspierany na serwerze, wymagany do instalacji i poprawnego działania oprogramowania zarządzającego wraz z niezbędnymi komponentami |

### 5.3.6 Serwery do backupu

Wykonawca jest zobowiązany do dostarczenia serwerów przeznaczonych do oprogramowania do zarządzania i wykonywania backupu. Serwery te będą działać w układzie klastra niezawodnościowego. Wraz z serwerami należy dostarczyć licencje na system operacyjny i oprogramowaniem klastra właściwy dla oprogramowania środowiska backupu.

Wymagania dla serwera do backupu typu rack:

| ID wymagania | Opis wymagania |
|---|---|

| | |
|---|---|
| INF.BLA.66. | Obudowa do montażu w szafie, wysokość maksymalna 2U, wymagane dostarczenie szyn montażowych do szafy, wysuwanego ramienia na kable oraz wszystkich innych niezbędnych elementów potrzebnych do instalacji i poprawnego działania serwera. |
| INF.BLA.67. | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| INF.BLA.68. | Procesory minimum sześciordzeniowy, x86 - 64 bity, osiągający w testach SPECint_rate2006 wynik nie gorszy niż 430 punktów dla konfiguracji testowej z dwoma procesorami. Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów |
| INF.BLA.69. | Minimum 2 zainstalowane procesory |
| INF.BLA.70. | Minimum min. 64GB pamięci RAM RDIMM. Serwer musi być wyposażony w min. 24 gniazd na moduły pamięci. Możliwość instalacji w serwerze min. 768GB RAM. Możliwość instalacji kości pamięci RDIMM lub UDIMM. |
| INF.BLA.71. | Minimum 6 slotów PCI-Express, w tym min. 1 sloty x16 (szybkość slotu – bus width) oraz minimum dwa sloty pełnej wysokości |
| INF.BLA.72. | Minimum 4 złącza typu 1GbEthernet RJ-45 |
| INF.BLA.73. | 8 interfejsów FC 8Gb. Minimum 4 karty FC zapewniająca minimum 2 interfejsy FC, każdy min. 8Gb |
| INF.BLA.74. | Wewnętrzne wnęki dyskowe przygotowane do instalacji i działania minimum ośmiu dysków SAS/SATA/SSD typu Hot-Plug. W serwerze zainstalowane min. 4 dyski twarde, każdy o parametrach: 300GB, prędkość obrotowa 10000 obrotów/minutę, SAS 6G, Hot-Plug. |
| INF.BLA.75. | Dedykowany kontroler RAID min 512MB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania. Możliwe konfiguracje 0, 1, 10, 5, 50 Możliwość rozbudowy wbudowanego w płytę kontrolera dyskowego o dodatkowe funkcje, takie jak RAID 6, 60. |
| INF.BLA.76. | Serwer wyposażony w wewnętrzny napęd DVD |
| INF.BLA.77. | Minimum 4 szt. portów USB, w tym jeden wewnętrzny. |
| INF.BLA.78. | Serwer wyposażony w kartę zdalnego zarządzania zapewniającą:<br>• Zdalne włączanie/wyłączanie/restart<br>• Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.<br>• Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.<br>• Podłączanie zdalnych napędów CD-ROM/DVD/ISO z możliwością bootowania z w/w napędów.<br>• Podgląd logów sprzętowych serwera i karty<br>• Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS).<br>• Obsługa Secured Shell, SSL, AES, RC4, dostęp z poziomu przeglądarki WWW jaki i z CLI , obsługa skryptów XML/PERL. |
| INF.BLA.79. | Zintegrowana karta graficzna. |
| INF.BLA.80. | 2 szt. zasilaczy, redundantne, hot plug. |
| INF.BLA.81. | Chłodzenie: redundantne, hot plug. |
| INF.BLA.82. | Możliwość zainstalowania modułu TPM na płycie głównej serwera ( w dedykowanym tylko dla tego modułu gnieździe/miejscu) |
| INF.BLA.83. | Wspierane systemy operacyjne: Microsoft Windows 2008R2 i 2012, Oracle Linux 6, Red Hat Enterprise Linux 6, SUSE Linux Enterprise Server 11, VMware ESXi 5. |
| INF.BLA.84. | Dostarczony system operacyjny: system operacyjny (OS ) wspierany na serwerze, wymagany do instalacji i poprawnego działania oprogramowania do wykonywania backupu wraz z niezbędnymi komponentami. |

### 5.3.7 Szafy serwerowe

Wymagania dla szafy serwerowej 19” z wyposażeniem dodatkowym:

| ID wymagania | Opis wymagania |
|---|---|

| | |
|---|---|
| INF.BLA.85. | Szafa serwerowa 19” o wewnętrznej przestrzeni do montażu urządzeń 42 U, zewnętrzne wymiar szafy:<br>• Wysokość max 201cm<br>• Szerokość max 60cm<br>• Głębokość max 113 cm.<br>• Obciążenie statyczne szafy nie mniejsze niż 1300kg<br>• Drzwi przednie perforowane (perforacja na poziomie min. 80%), drzwi tylnie dzielone – dwustronne. |
| INF.BLA.86. | Ściany boczne (zestaw). Ściany boczne zakładane i zdejmowane bez konieczności użycia narzędzi , każda ze ścian bocznych dzielona na min 3 panele.<br>Zestaw zaślepek (każda o wys. 1U, montowana bez użycia narzędzi) pozwalających na zasłonięcie min. 30 U wolnego miejsca w szafie.<br>Stabilizator (zestaw elementów stabilizujących szafę) zapobiegający wywróceniu szafy.<br>Zestaw elementów uziemiających.<br>Zestaw elementów umożliwiających automatycznie wykrywanie miejsca instalacji serwera w szafie i przekazywanie informacji do serwera. |
| INF.BLA.87. | Min. 2 PDU, każdy z zabezpieczeniem 32 A (moduły rozprowadzenia zasilania), zapewniające redundancję podłączenia zasilana do serwerów i obudów blade, razem dostarczające min. 8 gniazd C19 (16A) i min. 48 gniazd C13. |

## 5.4 Infrastruktura macierzowa

Wykonawca musi dostarczyć oraz uruchomić infrastrukturę macierzową, na którą składają się następujące elementy:

- Półki do macierzy operacyjnej (produkcyjnej)
- Półki do macierzy kopii zapasowych

### 5.4.1 Półki na dyski dla macierzy operacyjnej (produkcyjnej)

Wymagania minimalne:

| ID wymagania | Opis wymagania |
|---|---|
| INF.STO.1. | Musi być możliwość zainstalowania półki w szafie rack 19” |
| INF.STO.2. | Półka musi pochodzić od tego samego producenta co macierze zamawiane przez Zmawiającego w ramach 2. części 1. Zamówienia oraz posiadać tą samą wersję firmware’u co macierze, do której będzie podłączana. |
| INF.STO.3. | Dostarczona półka musi zostać zainstalowana w dostarczonej w ramach zadania 2. części 1. Zamówienia macierzy produkcyjnej, tak aby była widoczna jako natywny zasób tej macierzy |
| INF.STO.4. | Dostarczona półka musi zostać skonfigurowana zgodnie ze wymaganiami Zamawiającego w zakresie RAID oraz wolumenów fizycznych i logicznych |
| INF.STO.5. | Dostarczona półka musi zawierać niezbędne licencje rozszerzeń jeśli takie będą wymagane, w tym licencje na replikacje pozwalające na podłączenie jej do dostarczanej ramach zadania 2. części 1. Zamówienia macierzy |
| INF.STO.6. | Dostarczana półka musi być wyposażona w zasilanie z dwóch niezależnych źródeł zasilania. Zanik jednego z nich nie może powodować przerwy w pracy urządzenia ani zmniejszenia jego wydajności lub utraty danych. |
| INF.STO.7. | Każda z półek musi pozwalać na wymianę dysków podczas pracy systemu (Hot-Swap). |
| INF.STO.8. | Dostarczona półka musi zostać dostarczona z dyskami SATA/NL-SAS o pojemności co najmniej 36TB. |
| INF.STO.9. | Dyski muszą mieć pojemność co najmniej 2TB o prędkości obrotowej co najmniej 7,2K RPM. |

### 5.4.2 Półki na dyski dla macierzy kopii zapasowych

Wymagania minimalne:

| ID wymagania | Opis wymagania |
|---|---|
| INF.STO.10. | Musi być możliwość zainstalowania półki w szafie rack 19” |
| INF.STO.11. | Półka musi pochodzić od tego samego producenta co macierze zamawiane przez Zmawiającego w ramach zadania 2. części 1. Zamówienia oraz posiadać tą samą wersję firmware’u co macierze do której będzie podłączana. |
| INF.STO.12. | Dostarczona półka musi zostać zainstalowana w dostarczonej w ramach zadania 2. części 1. Zamówienia macierzy kopii zapasowych tak aby była widoczna jako natywny zasób tej macierzy. |
| INF.STO.13. | Dostarczona półka musi zostać zainstalowana w dostarczonej w ramach zadania 2. części 1. Zamówienia macierzy, tak aby była widoczna jako niezależny zasób tej macierzy. |
| INF.STO.14. | Dostarczona półka musi zostać skonfigurowana zgodnie ze wymaganiami Zamawiającego w zakresie RAID oraz wolumenów fizycznych i logicznych. |
| INF.STO.15. | Dostarczona półka musi zawierać niezbędne licencje rozszerzeń jeśli takie będą wymagane, w tym licencje na replikacje pozwalające na podłączenie jej do dostarczanej ramach zadania 2. części 1. Zamówienia macierzy. |
| INF.STO.16. | Dostarczana półka musi być wyposażona w zasilanie z dwóch niezależnych źródeł zasilania. Zanik jednego z nich nie może powodować przerwy w pracy urządzenia ani zmniejszenia jego wydajności lub utraty danych. |
| INF.STO.17. | Każda z półek musi pozwalać na wymianę dysków podczas pracy systemu (Hot-Swap). |
| INF.STO.18. | Dostarczona półka musi zostać dostarczona z dyskami SATA/NL-SAS o pojemności co najmniej 36TB. |
| INF.STO.19. | Dyski muszą mieć pojemność co najmniej 2TB o prędkości obrotowej co najmniej 7,2K RPM |

## 5.5 Infrastruktura bazodanowa

Infrastruktura bazodanowa składa się z serwera bazodanowego (DBMS) wraz z rozszerzeniami oraz urządzenia gwarantującego bezpieczeństwo danych.

### 5.5.1 Serwer bazodanowy (DBMS)

Świadczenie usługi dostępu do bazy danych w ramach Platformy wymaga rozwiązania skalowalnego i w pełni redundantnego w postaci klastra bazodanowego.

Wymagania ogólne dla oprogramowania klasy serwera bazodanowego (DBMS):

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.1. | Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla Itanium, Solaris dla procesorów SPARC/x86-64, IBM AIX), Intel Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach. |
| INF.DB.2. | Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych. |
| INF.DB.3. | Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego. |
| INF.DB.4. | Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji powinien pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, z kolei spójny odczyt nie powinien blokować możliwości wykonywania zmian. |
| INF.DB.5. | Oznacza to, że modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. |
| INF.DB.6. | Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). |
| INF.DB.7. | Możliwość migracji 8-bitowego zestawu znaków bazy danych (np MS Windows CP 1252, ISO 8859-2) do Unicode. |

| | |
|---|---|
| INF.DB.8. | Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych. |
| INF.DB.9. | Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). |
| INF.DB.10. | Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. |
| INF.DB.11. | Możliwość kompilacji procedur składowanych w bazie danych do postaci kodu binarnego. |
| INF.DB.12. | Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). |
| INF.DB.13. | W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek. |
| INF.DB.14. | Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań. |
| INF.DB.15. | Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. |
| INF.DB.16. | Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, Data Protector itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online. |
| INF.DB.17. | Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup). |
| INF.DB.18. | Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. |
| INF.DB.19. | W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników. |
| INF.DB.20. | Możliwość przeprowadzenia odtwarzania na poziomie pojedynczych bloków danych. Pozostałe bloki w uszkodzonym pliku pozostają dostępne dla użytkowników. |
| INF.DB.21. | Możliwość zaimplementowania polityki bezpieczeństwa regulującej dostęp do danych na poziomie pojedynczych wierszy w tabelach. Mechanizm ten powinien być realizowany za pomocą mechanizmów motoru bazy danych i powinien być przezroczysty dla aplikacji. |
| INF.DB.22. | Motor bazy danych powinien udostępniać możliwość zrównoleglenia operacji SQL (zapytania, instrukcje DML, ładowanie danych, tworzenie indeksów, przenoszenie tabel/indeksów pomiędzy przestrzeniami danych) oraz procesów wykonywania kopii bezpieczeństwa bądź odtwarzania. |
| INF.DB.23. | Motor bazy danych powinien umożliwiać wykonywanie niektórych operacji związanych z utrzymaniem bazy danych bez konieczności pozbawienia dostępu użytkowników do danych. W szczególności dotyczy to tworzenia / przebudowywania indeksów oraz reorganizacji bądź |

| | |
|---|---|
| | redefinicji tabel. |
| INF.DB.24. | Możliwość zakładania/przebudowywania indeksów online bez konieczności odłączenia użytkowników operujących (zapytania, operacje insert, update, delete) na tabelach podlegających indeksowaniu. |
| INF.DB.25. | Możliwość zarządzania przydziałem zasobów obliczeniowych dla użytkowników bazy danych (Resource Manager). |
| INF.DB.26. | Wsparcie dla typu danych DICOM obsługiwanego wewnętrznie przez serwer bazy danych. |
| INF.DB.27. | Możliwość zakładania w tabelach kolumn typu obsługującego standard DICOM. |
| INF.DB.28. | Możliwość przeszukiwania zakładania indeksów na grupie atrybutów metadanych składowanych w kolumnach przechowujących dane w formacie DICOM. |
| INF.DB.29. | Możliwość przeszukiwania metadanych:<br>• wszystkich bądź niektórych atrybutów,<br>• możliwość zakładania indeksów na wybranych atrybutach,<br>• możliwość wyszukiwania pełnotekstowego,<br>• możliwość nawigacji zgodnej z hierarchią atrybutów. |
| INF.DB.30. | Składowanie metadanych DICOM i treści DICOM odbywa się wewnątrz bazy danych. |
| INF.DB.31. | Operowanie na danych DICOM za pomocą konstrukcji języka SQL, procedur składowanych, dostęp za pomocą Java API. |
| INF.DB.32. | Wbudowane mechanizmy konwersji treści DICOM do formatów JPEG, GIF, MPEG, AVI. |
| INF.DB.33. | Możliwość zwiększenia przepustowości bazy danych poprzez uruchomienie dodatkowych serwerów obsługujących tą samą bazę danych (w klastrze). |
| INF.DB.34. | Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej (zmiana organizacji plików danych) oraz logicznej struktury baz danych (tabel / indeksów). |
| INF.DB.35. | Unieruchomienie jednego z serwerów bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów |
| INF.DB.36. | Możliwość kontynuacji pracy użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Powinna istnieć możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia. |
| INF.DB.37. | Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera do którego zostało nawiązane połączenie |
| INF.DB.38. | Na całość dostarczonego sprzętu zostanie udzielona gwarancja na okres 12 miesięcy wraz z 12-to miesięczna usługą wsparcia technicznego |

### 5.5.2 Opcje dodatkowe serwera bazodanowego

W ramach zintegrowanej platformy bazodanowej Wykonawca musi dostarczyć opcje (dodatkowe funkcjonalności) wspierające:

- Działanie bazy danych w klastrze bazodanowym
- Zaawansowane opcje bezpieczeństwa, np. możliwość szyfrowania komunikacji
- Raportowanie
- Partycjonowanie
- Diagnozowanie wydajności bazy danych
- Dostrojenie bazy danych
- Automatyzację procesów uaktualnienia oprogramowania bazodanowego
- Umożliwienie świadczenia usług w chmurze
- Umożliwienie kompresji i deduplikacji danych

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.39. | Wszystkie rozszerzenia (opcje) muszą działać w ramach zintegrowanej platformy bazodanowej. |

| | |
|---|---|
| | Oznacza to, że wykorzystywane mogą być tylko zasoby wbudowane w zintegrowaną platformę bazodanową. |

Wymagania w zakresie działania bazy danych w klastrze bazodanowym:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.40. | Możliwość zwiększenia przepustowości bazy danych poprzez uruchomienie dodatkowych serwerów obsługujących tą samą bazę danych (w klastrze). |
| INF.DB.41. | Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej (zmiana organizacji plików danych) oraz logicznej struktury baz danych (tabel / indeksów). |
| INF.DB.42. | Unieruchomienie jednego z serwerów bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów |
| INF.DB.43. | Możliwość kontynuacji pracy użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Powinna istnieć możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia. |
| INF.DB.44. | Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera do którego zostało nawiązane połączenie |

Wymagania w zakresie bezpieczeństwa:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.45. | Możliwość szyfrowania transmisji pomiędzy aplikacją a serwerem bazy danych przezroczysta dla aplikacji. |
| INF.DB.46. | Szyfrowanie transmisji musi być możliwe w oparciu o algorytmy z użyciem klucza symetrycznego (DES, 3DES, AES), z zapewnieniem integralności transmisji, uwierzytelnienia stron oraz bezpiecznej wymiany kluczy. |
| INF.DB.47. | Przezroczyste dla aplikacji szyfrowanie danych składowanych na nośnikach dyskowych. Szyfrowaniu powinny podlegać wskazane pliki danych. |
| INF.DB.48. | Możliwość składowania klucza do bazy danych w wyspecjalizowanym urządzeniu sprzętowym (HSM - hardware security module), odpornym na próby wydobycia klucza na zewnątrz urządzenia. |

Wymagania w zakresie raportów:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.49. | Rozwiązanie musi dostarczać wiedzy w obszarze bieżących ustawień bezpieczeństwa w bazie danych, prezentowanej w formie specjalistycznych raportów |
| INF.DB.50. | Rozwiązanie musi się integrować z narzędziem graficznym do zarządzania bazą, tak aby wykonywanie odpowiedniej konfiguracji możliwe było z wykorzystaniem narzędzi graficznych, a dystrybucja ustawień realizowana jednocześnie dla wielu baz |
| INF.DB.51. | Rozwiązanie musi realizować funkcjonalność ochrony dowolnej tabeli przed użytkownikami administracyjnymi, posiadającymi najwyższe systemowe uprawnienia (np. select_any_table), tak aby nie było możliwości odczytania informacji |
| INF.DB.52. | Rozwiązanie musi realizować koncepcję rozdziału uprawnień (tzw. Separation of Duties) w bazie danych |
| INF.DB.53. | Rozwiązanie powinno być konfigurowalne dla osobnych instancji bazy, jak również dla konfiguracji skonfigurowanych jako klaster |
| INF.DB.54. | Rozwiązanie musi realizować funkcjonalność grupowania obiektów, które będą zabezpieczone, tak aby możliwe było zgrupowanie schematy bazy, dowolnej tabeli, dowolnego obiektu w bazie w jeden logiczny byt |
| INF.DB.55. | Rozwiązanie musi pozwalać kontrolować każdą operację SQL wykonywaną przez użytkownika w bazie danych. Musi istnieć możliwość wpływania czy określone operacje (takie jak ALTER SYSTEM, operacje DDL, operacje DML) mają być wykonane przez użytkownika, czy nie, pomimo |

| | |
|---|---|
| | posiadanych przez niego uprawnień w bazie. |
| INF.DB.56. | Rozwiązanie musi pozwalać na określenie dodatkowych warunków uwierzytelniania lub wykonania operacji na bazie, tak aby realizacja określonych działań w bazie możliwa była tylko w godzinach pracy, z określonej adresacji IP. |
| INF.DB.57. | Rozwiązanie musi realizować koncepcję właściciela biznesowego informacji, czyli pozwolić na kontrolę informacji w taki sposób, aby dostęp do informacji nie był możliwy poza politykami dostępu zaakceptowanymi przez właściciela informacji |
| INF.DB.58. | Rozwiązanie powinno móc wykorzystać mechanizm klasyfikacji informacji, czyli określenie dostępu do obiektów bazy na podstawie wartości informacji |
| INF.DB.59. | Rozwiązanie musi pozwalać na raportowanie wszystkich prób naruszenia w obszarze szczególnie chronionym (np. próba nieuprawnionego dostępu do tabeli płac) |
| INF.DB.60. | Rozwiązanie musi umożliwiać odebranie najwyższych uprawnień roli administracyjnej (np. DBA). Jako najwyższe uprawnienia rozumiane są np. 'select any transaction', 'create any job' itd |

Wymagania w zakresie partycjonowania:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.61. | Możliwość fizycznego umieszczenia wierszy tabeli w wielu niezależnych segmentach (partycjach) na podstawie wartości kluczy. Podział danych musi być przezroczysty dla aplikacji (instrukcji SQL). |
| INF.DB.62. | Możliwość szybkiego podziału segmentu na mniejsze partycje oraz możliwość scalenia wielu partycji w jedną partycję. |
| INF.DB.63. | Możliwość wyboru różnych strategii partycjonowania – wg zakresu wartości atrybutów, wg klucza haszującego lub wg listy wartości atrybutów. |
| INF.DB.64. | W przypadku, gdy w instrukcji SQL są podane warunki równości lub zakresowe dotyczące kluczy partycjonowania, optymalizator SQL powinien umożliwić przetwarzanie danych wyłącznie z tych segmentów (partycji), w których leżą dane wymagane do realizacji instrukcji SQL. |
| INF.DB.65. | Dostępność wielu strategii indeksowania spartycjonowanych tabel. Powinna istnieć możliwość założenia dużego indeksu na spartycjonowanej tabeli (jedno B*drzewo lub jedna mapa bitowa na całą spartycjonowaną tabelę), możliwość założenia indeksów spartycjonowanych, odzwierciedlających schemat partycjonowania tabeli, bądź indeksu spartycjonowanego, którego schemat partycjonowania jest odmienny niż schemat partycjonowania w tabeli. |

Wymagania w zakresie diagnozowania wydajności bazy danych:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.66. | Rozszerzenie do bazy danych powinno zapewniać automatyczne diagnozowanie wydajności i wąskich gardeł w konfiguracji bazy danych na podstawie prekonfigurowanych i możliwych do modyfikacji parametrów (np. obciążenie procesora, zajętość dysków itp.) oraz konfigurowalne powiadamianie o odchyleniach od wartości oczekiwanej. |

Wymagania w zakresie dostrojenia bazy danych:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.67. | Rozszerzenie do bazy danych powinno zapewniać mechanizmy do analizy zapytań wykonywanych w bazie danych oraz obiektów bazy danych oraz proponować na podstawie przeprowadzonej analizy dostrojenie nieoptymalnych zapytań używanych w bazie danych oraz reorganizację obiektów bazy danych (tabele, indeksy). |

Wymagania w zakresie automatyzacji procesów uaktualnienia oprogramowania bazodanowego:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.68. | Część funkcjonalna lub rozszerzenie serwera bazy danych, działająca na platformach sprzętowych i systemowych wspieranych przez bazę danych; pozwalająca na automatyzację |

| | |
|---|---|
| | procesów uaktualnienia oprogramowania bazodanowego na wielu serwerach oraz analizy procesu uaktualnień. |
| INF.DB.69. | Możliwość automatycznego gromadzenia parametrów konfiguracji baz danych ich porównywania oraz wykonywania raportów porównawczych z różnych okresów. |
| INF.DB.70. | Przechowywanie historii konfiguracji. |
| INF.DB.71. | Możliwość automatycznego wykrywania nowych instalacji baz danych w środowisku i objęcia ich stosownym monitoringiem. |
| INF.DB.72. | Możliwość przechowywania topologii infrastruktury oraz jej wizualizacji w postaci mapy topologii wraz z możliwością dodania relacji pomiędzy obiektami. |
| INF.DB.73. | Wsparcie dla procesu uaktualnienia baz danych metodą „Out-of-Place Patching” |
| INF.DB.74. | Możliwość porównywania danych pomiędzy dwoma bazami danych. |
| INF.DB.75. | Możliwość synchronizacji kodu PLSQL pomiędzy bazami danych. |
| INF.DB.76. | Wsparcie procesu dostarczania infrastruktury bazodanowej na wielu serwerach z określonym uprzednio standardem. |
| INF.DB.77. | Wsparcie procesu klonowania środowisk bazodanowych. |
| INF.DB.78. | Wsparcie procesu migracji baz danych z wersji samodzielnej do wersji klastrowej. |

Wymagania w zakresie umożliwienia świadczenia usług w chmurze:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.79. | Możliwość utworzenia infrastruktury chmury |
| INF.DB.80. | Możliwość zarządzania infrastrukturą chmury poprzez dedykowany interfejs |
| INF.DB.81. | Możliwość utworzenia specjalnego portalu dla administratorów infrastruktury chmury |
| INF.DB.82. | Możliwość rozliczalności ze zużytych zasobów przez odbiorców infrastruktury w środowisku chmury |
| INF.DB.83. | Możliwość tworzenia planów konsolidacji obecnego środowiska do chmury |

Wymagania w zakresie kompresji i deduplikacji danych:

| ID wymagania | Opis wymagania |
|---|---|
| INF.DB.84. | Funkcjonalność kompresji jest funkcjonalnością wbudowaną niewymagająca rozbudowy przy pomocy zewnętrznych narzędzi programistycznych. |
| INF.DB.85. | Funkcjonalność kompresji musi być funkcjonalnością oprogramowania bazodanowego niezależną od systemu operacyjnego na którym pracuje oprogramowanie baz danych. |
| INF.DB.86. | Rozwiązanie dostarcza funkcjonalności kompresji danych znajdujących się w tabelach bazy danych. Użyty algorytm kompresji nie powinien degradować wydajności aplikacji o charakterze pracy OLTP. |
| INF.DB.87. | Użyty mechanizm kompresji nie powinien uniemożliwiać operacji DML na bazie danych. Operacje DML nie powinny wpływać na poziom kompresji danych w tabeli. |
| INF.DB.88. | Użyty mechanizm kompresji nie powinien wymuszać specjalnego trybu ładowania/uaktualniania danych do/w tabeli. |
| INF.DB.89. | Rozwiązanie dostarcza funkcjonalności kompresji eksportów logicznych bazy danych. |
| INF.DB.90. | Rozwiązanie dostarcza funkcjonalności kompresji danych niestrukturalnych przechowywanych w bazie danych. Dane takie przechowywane są zazwyczaj jako tzw. wielkie obiekty - LOB. Funkcjonalność kompresji danych niestrukturalnych powinna mieć możliwość konfiguracji wykorzystanego algorytmu kompresji. Dostępne powinny być przynajmniej trzy poziomy kompresji danych przechowywanych w bazie danych jako obiekty LOB. |
| INF.DB.91. | Rozwiązanie dostarcza funkcjonalności deduplikacji danych niestrukturalnych przechowywanych w bazie danych. Dane takie przechowywane są zazwyczaj jako tzw. wielkie obiekty - LOB. Funkcjonalność deduplikacji obiektów LOB pozwala na zmniejszenie przestrzeni potrzebnej na przechowywanie ich w bazie danych optymalizując powtarzające się fragmenty danych w wielkim obiekcie. |
| INF.DB.92. | Rozwiązanie dostarcza funkcjonalności kompresji transmisji pomiędzy baza danych podstawowa a baza danych pozostającą w trybie tzw. standby znajdującą się w ośrodku zapasowym w celu |

| | |
|---|---|
| | obniżenia wymagań na pasmo pomiędzy ośrodkiem podstawowym a ośrodkiem zapasowym. |
| INF.DB.93. | Rozwiązanie dostarcza funkcjonalności kompresji kopii zapasowych (backup) bazy danych. Kompresja kopii zapasowych musi odbywać się od razu w czasie tworzenia kopii zapasowej. Funkcjonalność kompresji kopii zapasowych powinna mieć możliwość konfiguracji wykorzystanego algorytmu kompresji. W zależności od użytego algorytmu użytkownik może sterować zależnością pomiędzy współczynnikiem kompresji, wykorzystaniem CPU, czasem wykonania kopii zapasowej. Mechanizm kompresji kopii zapasowych musi dostarczać przynajmniej trzech poziomów kompresji. |
| INF.DB.94. | Rozwiązanie dostarcza funkcjonalności kompresji transmisji pomiędzy baza danych a aplikacją. |
| INF.DB.95. | Rozwiązanie dostarcza funkcjonalności automatycznej implementacji zarządzania cyklem życia danych (ILM – Information Lifecycle Management). Dla danych często wykorzystywanych stosowany jest algorytm kompresji nie pogarszający wydajności pracy bazy danych w trybie OLTP. Dane archiwalne są automatycznie kompresowane silnymi algorytmami kompresji, mogą być w trybie online (bez wpływu na pracę użytkowników) przenoszone na inną warstwę storage (Automated Tiered Storage). |
| INF.DB.96. | Rozwiązanie dostarcza funkcjonalności śledzenia wykonywanych operacji SQL i DML na tabelach i partycjach tabel. |
| INF.DB.97. | Rozwiązanie dostarcza funkcjonalności wsparcia wykonywania kopii zapasowych z udziałem mechanizmów dostępnych na macierzach dyskowych np. tworzenia tzw. snapshot lub clone. |
| INF.DB.98. | Rozwiązanie dostarcza funkcjonalności przeniesienia partycji tabel w trybie online przy czym przeniesienie partycji może być połączone z kompresją danych. |

### 5.5.3 System SIEM dla ochrony środowiska bazodanowego

Urządzenie klasy SIEM (Security information and event management) dla ochrony środowiska bazodanowego. Urządzenie musi umożliwić realizację co najmniej poniższych funkcji:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BEZP.DB.1. | Rozwiązanie musi umożliwiać monitorowanie ruchu SQL do baz danych, w szczególności zintegrowanej platformy bazodanowej oraz co najmniej następujących rozwiązań:<br>• Oracle DB,<br>• IBM DB2,<br>• Microsoft SQL minimum w wersji 2005. |
| INF.BEZP.DB.2. | Rozwiązanie musi monitorować wszystkie żądania typu SELECT, DML, DDL i DCL zarówno inicjowane zdalnie jak i lokalnie włącznie z protokołami: Bequeath i IPC |
| INF.BEZP.DB.3. | System musi mieć możliwość analizy wywołań procedur składowanych z możliwością identyfikacji obiektów modyfikowanych przez procedurę wspomnianych procedur składowanych |
| INF.BEZP.DB.4. | Rozwiązanie musi audytować szczegółowe informacje na poziomie sesji (adresy IP, oprogramowanie nawiązanie sesji, protokół, użytkownika), zapytania (składnię, parametry wywołania) |
| INF.BEZP.DB.5. | Monitorowane informacje muszą podlegać analizie z użyciem polityk umożliwiając:<br>a) blokowanie określonego ruchu<br>b) zachowanie informacji dla celów śledczych<br>c) notyfikację określonych użytkowników |
| INF.BEZP.DB.6. | System musi normalizować dane dla celów śledczych i przechowywać je w relacyjnej bazie danych |
| INF.BEZP.DB.7. | System musi umożliwiać monitorowanie połączeń szyfrowanych do systemu Exadata z użyciem ASO lub SSL |
| INF.BEZP.DB.8. | System musi być wyposażony w moduł raportowy umożliwiający na samodzielną budowę zapytań i definicję formy prezentacji informacji (tabele, wykresy) |
| INF.BEZP.DB.9. | Raportowanie musi umożliwiać na budowę raportów zbiorczych dla danych audytowych pochodzących z różnych źródeł (różne instancje zintegrowanej platformy bazodanowej) |
| INF.BEZP.DB.10. | System powinien być wyposażony w moduł klasyfikacji danych pozwalający na wyszukiwanie danych wrażliwych w oparciu o wzorce. Powinien posiadać możliwość |

| | |
|---|---|
| | definiowania własnych metod analizy nie ograniczony jedynie do wyrażeń regularnych |
| INF.BEZP.DB.11. | System musi kontrolować stan konfiguracji środowiska zintegrowanej platformy bazodanowej poprzez identyfikację zmian zarówno dla kluczowych elementów silnika jak i systemu operacyjnego |
| INF.BEZP.DB.12. | System musi być posiadać wbudowany moduł szacowania podatności dla silnika zintegrowanej platformy bazodanowej bazujący na aktualizowanej liście publicznie znanych podatności oraz kontrolujący stan utwardzenia systemu zgodny przynajmniej ze standardem przemysłowym STIG |
| INF.BEZP.DB.13. | System musi posiadać moduł kontroli uprawnień do danych na poziomie silnika bazodanowego identyfikujący zmiany w uprawnieniach i pozwalający raportować ich stan w określonym czasie wstecz |
| INF.BEZP.DB.14. | System musi umożliwiać korelowanie zdarzeń w oparciu o zdefiniowane progi wystąpienie zdarzeń lub kolejności ich wystąpienia. Korelacja musi bazować na wszystkich danych zbieranym przez rozwiązanie (pochodzące z wszystkich monitorowanych środowisk zintegrowanej platformy bazodanowej). |
| INF.BEZP.DB.15. | System powinien umożliwiać budowanie procesu zarządzania incydentem wywoływanym na poziomie polityk lub incydentów z możliwością przekazywania podgrupy zdarzeń do określonych właścicieli danych. Proces zarządzania incydentem musi identyfikować przynajmniej dwie niezależne role audytora oraz właściciela incydentu i w zależności od roli wymuszać określone akcje -akceptacja, zdefiniowanie wyjątku, wyjaśnienie, delegacja do innej osoby. |

## 5.6 Infrastruktura programowa

### 5.6.1 Platforma wirtualizacyjna

Platforma wirtualizacyjna oraz oprogramowanie zarządzające wirtualizacją muszą pozwalać na utworzenie i zarządzanie środowiskiem wirtualnym.

Dostarczone oprogramowanie musi spełniać poniższe wymagania.

| ID wymagania | Opis wymagania |
|---|---|
| WIRT.1 | Oprogramowanie musi umożliwiać uruchamianie wirtualizacji na serwerach fizycznych o łącznej liczbie wskazanej w zestawieniu ilościowym. |
| WIRT.2 | Zarządzanie wszystkimi zwirtualizowanymi zasobami musi odbywać się przy użyciu jednej konsoli do zarządzania całym środowiskiem. |
| WIRT.3 | Oprogramowanie musi pozwalać na wydzielenie środowiska produkcyjnego, testowego i deweloperskiego w warstwie wirtualnej z użyciem wirtualizatora z wykorzystaniem mechanizmu pól zasobów (resource pool). Środowiska te nie mogą być wydzielone fizycznie. |
| WIRT.4 | Oprogramowanie musi pozwalać na integrację z oprogramowaniem do zarządzania infrastrukturą |
| WIRT.5 | Oprogramowanie musi pozwalać na przenoszenie aplikacji pomiędzy środowiskami z zachowaniem stabilności środowisk i mechanizmu anonimizacji danych |
| WIRT.6 | Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym. |
| WIRT.7 | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| WIRT.8 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 1TB pamięci operacyjnej. |
| WIRT.9 | Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym 32 procesorów wirtualnych. |
| WIRT.10 | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. |

| | |
|---|---|
| WIRT.11 | Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| WIRT.12 | Rozwiązanie musi wspierać następujące systemy operacyjne:<br>• Windows XP,<br>• Windows Vista,<br>• Windows Server 2003,<br>• Windows Server 2008,<br>• Windows Server 2008 R2,<br>• Windows Server 2012,<br>• SLES 11,<br>• SLES 10,<br>• SLES9,<br>• SLES8,<br>• Ubuntu 13.04,<br>• Ubuntu 12.04 LTS,<br>• Oracle Linux 5,<br>• Oracle Linux 6,<br>• RHEL 5,<br>• RHEL 4,<br>• RHEL 3,<br>• RHEL 2.1,<br>• Solaris wersja 10 dla platformy x86,<br>• NetWare 6.5,<br>• NetWare 6.0,<br>• NetWare 6.1,<br>• Debian,<br>• CentOS,<br>• FreeBSD,<br>• Asianux,<br>• SCO OpenServer,<br>• SCO Unixware,<br>• Mac OS X. |
| WIRT.13 | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągniecia maksymalnego współczynnika konsolidacji. |
| WIRT.14 | Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi usługami. |
| WIRT.15 | Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej. |
| WIRT.16 | Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie. |
| WIRT.17 | Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. |
| WIRT.18 | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. |
| WIRT.19 | Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek. |
| WIRT.20 | Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni. |
| WIRT.21 | Rozwiązanie musi umożliwiać udostepnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane. |
| WIRT.22 | Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości 64TB |
| WIRT.23 | System musi umożliwiać tworzenie standardowej konfiguracji dla hostów i zautomatyzowanie zgodności dla tych konfiguracji. |

| | |
|---|---|
| WIRT.24 | System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE |
| WIRT.25 | System musi mieć możliwość tworzenia wirtualnego przełącznika, którego konfiguracja administrowana jest centralnie z poziomu konsoli zarządzającej. Pojedynczy przełącznik wirtualny musi mieć możliwość obsługiwania więcej niż jednego hosta fizycznego. |
| WIRT.26 | Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. |
| WIRT.27 | System musi mieć możliwość przenoszenia plików wirtualnych maszyn pomiędzy zasobami dyskowymi bez potrzeby wyłączania wirtualnych maszyn. |
| WIRT.28 | Rozwiązanie musi zapewnić ciągłą pracę usług. Usługi krytyczne biznesowo muszą działać bez przestoju, czas niedostępności innych usług nie powinien przekraczać kilkunastu minut. |
| WIRT.29 | Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury. |
| WIRT.30 | Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. |
| WIRT.31 | Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. |
| WIRT.32 | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak, aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany. |
| WIRT.33 | Rozwiązanie musi zapewnić możliwość szybkiego wykonywania kopii zapasowych oraz odtwarzania usług. Proces ten nie powinien mieć wpływu na utylizację zasobów fizycznych infrastruktury wirtualnej. |
| WIRT.34 | Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych. |
| WIRT.35 | Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych systemów. |
| WIRT.36 | Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Pożądana jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi oraz wolumenami dyskowymi, bez przerywania pracy usług. |
| WIRT.37 | Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia serwerów fizycznych pracujących jak platforma dla infrastruktury wirtualnej. |
| WIRT.38 | System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju |
| WIRT.39 | System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn |
| WIRT.40 | System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką |
| WIRT.41 | System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone. |

### 5.6.2 Serwer aplikacji

Serwer aplikacji stanowi podstawowy element środowiska aplikacji i zakłada się, że aplikacje biznesowe oraz infrastrukturalne będą domyślnie na nim osadzone. Odstępstwa są dopuszczone jedynie w przypadku niezgodności środowiska (np. JEE a .Net) oraz przy zgodzie Zamawiającego.

Wymagania w zakresie obsługiwanych standardów:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AS.1. | Infrastruktura serwera aplikacji musi posiadać wsparcie dla Java SE wersja 6 |
| INF.AS.2. | Infrastruktura serwera aplikacji musi być certyfikowaną platformą w zgodzie ze standardem Java EE wersja 5 |
| INF.AS.3. | Infrastruktura serwera aplikacji musi być certyfikowaną platformą wobec Spring Framework |
| INF.AS.4. | Infrastruktura serwera aplikacji musi posiadać wbudowaną integrację EJB 3.0 i Spring |
| INF.AS.5. | Infrastruktura serwera aplikacji musi posiadać wbudowane wsparcie dla specyfikacji Commons J Work Manager API i Timer API |
| INF.AS.6. | Infrastruktura serwera aplikacji musi posiadać wbudowane wsparcie dla specyfikacji JSR-88 – plany wdrożeń (Deployment Plan) |
| INF.AS.7. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardu Web services WS-ReliableMessaging 1.1 i WS-ReliableMessaging Policy 1.1 |
| INF.AS.8. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardu Web services WS-Trust 1.3 |
| INF.AS.9. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardu Web services WS-SecureConversation 1.3 |
| INF.AS.10. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardu Web services WS-Security 1.1 |
| INF.AS.11. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardu Web services WS-SecurityPolicy 1.2 |
| INF.AS.12. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardu Web Service MTOM\XOP – SOAP Message Transmission Optimization Mechanism/XML-binary Optimized Packaging |
| INF.AS.13. | Wymagane jest wsparcie producenta dla środowiska uruchomieniowego serwera aplikacji niezależnie od wsparcia dla oprogramowania samego serwera aplikacji |

Wymagania w zakresie obsługi standardów bezpieczeństwa:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AS.14. | Infrastruktura serwera aplikacji musi posiadać możliwość realizacji odpowiedniego poziomu bezpieczeństwa w zakresie:<br>• uwierzytelniania<br>• kontroli dostępu<br>• zarządzania użytkownikami, grupami i rolami<br>• tworzenia, przechowywania i walidacji certyfikatów, haseł, kluczy<br>• audytowania zdarzeń bezpieczeństwa<br>• wsparcia dla mechanizmu pojedynczego logowania SSO |
| INF.AS.15. | Infrastruktura serwera aplikacji musi dostarczać mechanizmy uwierzytelniania i szyfrowania usług takie jak: użytkownik/hasło, passphrase, weryfikacja hostów, brak uwierzytelniania, tunelowanie wywołań SSL, certyfikaty X.509 |
| INF.AS.16. | Infrastruktura serwera aplikacji musi posiadać wbudowaną, dostępną poprzez konfigurację, integrację z katalogami użytkowników, grup i ról – LDAP, Active Directory, bazy danych, Windows NT, X.509, SAML, własne |
| INF.AS.17. | Infrastruktura serwera aplikacji musi posiadać możliwość jednoczesnego podłączenia wielu usług katalogowych, w tym różnego typu (np. równocześnie LDAP, Active Directory, bazy danych, Web service, systemy autentykacji i autoryzacji firm trzecich, własne) |
| INF.AS.18. | Infrastruktura serwera aplikacji musi posiadać opisaną w dokumentacji (wraz z przykładami) możliwość tworzenia własnych implementacji usług security: uwierzytelnienia, autoryzacji, mapowania ról, mapowania uwierzytelnień, baz danych kluczy/certyfikatów, walidacji poprawności kluczy/certyfikatów (CLV/CLR), audytowania, itd. |
| INF.AS.19. | Infrastruktura serwera aplikacji musi posiadać obsługę specyfikacji:<br>- Java Authentication and Authorization Service (JAAS), |

| | |
|---|---|
| | - Java Secure Sockets Extensions (JSSE),<br>- Java Cryptography Extensions (JCE),<br>- Java Authorization Contract for Containers (JACC) |
| INF.AS.20. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardów SAML 1.1, SAML 2.0 lub wyższych |
| INF.AS.21. | Infrastruktura serwera aplikacji musi posiadać wbudowaną integrację w ramach Single-Sign-On (SSO) z takimi technologiami jak SAML (1.1, 2.0), Kerberos (SPENEGO, Windows 2000 i 2003, .NET), Web service (SAML) |
| INF.AS.22. | Infrastruktura serwera aplikacji musi posiadać wbudowane API do funkcjonalności przeszukiwania i walidacji certyfikatów X.509 (CLV – Certificate Lookup and Validation) |
| INF.AS.23. | Infrastruktura serwera aplikacji musi posiadać obsługę mechanizmów autoryzacji i mapowania ról przy użyciu standardu XACML 2.0 |
| INF.AS.24. | Infrastruktura serwera aplikacji musi posiadać możliwość konfiguracji dynamicznego członkowstwa ról, np. uwzględniającego datę i czas, zawartość wybranych elementów w komunikatach SOAP (Web services), wartość atrybutów żądań HTTP, wartość atrybutów sesji HTTP, czy parametrów metod EJB |
| INF.AS.25. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę protokołu SNMP v3 wraz z HMAC-MD5-96, HMAC-SHA-96 |

Wymagania w zakresie realizacji wydajności oraz mechanizmów wysokiej dostępności:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AS.26. | Infrastruktura serwera aplikacji musi posiadać publicznie dostępne raporty (benchmarki) dotyczące wydajności serwera aplikacyjnego (np. Spec Java Application Server). Raporty powinny zawierać szczegółowe informacje o zastosowanej konfiguracji serwera aplikacyjnego, JVM, bazy danych, sprzętu i innych komponentów użytych podczas testowania. Raporty muszą znajdować się na stronach WWW organizacji powołanych do ustanawiania i publikowania standardowych benchmarków wydajnościowych. Ponadto raporty muszą być publikowane na stronach WWW nie związanych z Wykonawcą lub Oferentem. |
| INF.AS.27. | Infrastruktura serwera aplikacji musi posiadać wbudowane automatyczne samostrojenie się serwera aplikacyjnego (self-tuning) |
| INF.AS.28. | Infrastruktura serwera aplikacji musi posiadać wbudowaną możliwość klastrowania połączeń JDBC |
| INF.AS.29. | Infrastruktura serwera aplikacji musi posiadać wbudowaną możliwość klastrowania JMS (w tym automatyczne przełączanie klientów JMS w momencie failover serwerów JMS) |
| INF.AS.30. | Infrastruktura serwera aplikacji musi posiadać możliwość klastrowania obiektów typu singelton w aplikacjach |
| INF.AS.31. | Infrastruktura serwera aplikacji musi posiadać obsługę klastrowania dla mechanizmu Store-and-Forward |
| INF.AS.32. | Infrastruktura serwera aplikacji musi posiadać obsługę klastrowania Web-services zgodnych z WS-ReliableMessaging |

Wymagania w zakresie infrastruktury serwera aplikacji:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AS.33. | Infrastruktura serwera aplikacji musi posiadać wbudowane wsparcie dla współdzielenia kodu (np. bibliotek) pomiędzy wieloma aplikacjami (Web, EJB, Web services). Biblioteki (JAR, WAR, EAR, EJB) powinny być instalowane w serwerze aplikacyjnym jednokrotnie i wiele aplikacji może z nich skorzystać. Możliwość zainstalowania wielu wersji bibliotek równocześnie. |
| INF.AS.34. | Możliwość konfiguracji, która wersja biblioteki będzie wykorzystywana przez aplikację. Konfiguracja powinna odbywać się w sposób deklaratywny (za pomocą deployment deskryptor'ów) – nie poprzez kopiowanie kodu bibliotek do aplikacji. Przykład – wiele implementacji JSF działających równocześnie w serwerze aplikacyjnym |
| INF.AS.35. | Infrastruktura serwera aplikacji musi posiadać możliwość konfiguracji komponentów w aplikacjach webowych (np. servletów, filtrów servletów, web services) za pomocą adnotacji |

| | |
|---|---|
| | (ang. Annotations) Java (dotyczy także parametrów specyficznych dla danego serwera aplikacyjnego) |
| INF.AS.36. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę żądań HTTP w sposób asynchroniczny (czyli możliwość rozdzielenia obsługi HTTP request i HTTP response na różne wątki) |
| INF.AS.37. | Infrastruktura serwera aplikacji musi posiadać wbudowane wsparcie dla przechowywania (persistence) sesji webowych i EJB w pliku, bazie danych i pamięci |
| INF.AS.38. | Infrastruktura serwera aplikacji musi posiadać możliwość przechowywania istotnych informacji dotyczących sesji użytkownika (w tym sesja http, konteksty usług typu Servlet oraz konteksty usług typu Session EJB) w zewnętrznej pamięci cache poza głównym procesem maszyny wirtualnej Java. Oprogramowanie musi umożliwiać mechanizmy klastrowania aplikacji w powyższy sposób, czyli z wykorzystaniem cache'a zewnętrznego |
| INF.AS.39. | Infrastruktura serwera aplikacji musi posiadać wsparcie dla replikacji sesji w pamięci pomiędzy wieloma instancjami serwerów aplikacyjnych uruchomionych na wielu fizycznych maszynach. Replikacja sesji powinna zapewniać wysoką wydajność, w tym możliwość replikowania sesji w trybie primary-secondary (czyli zarządzanie maksymalnie dwiema kopiami sesji użytkownika w klastrze), replikowanie sesji z użyciem trybów IP unicast i multicast, a także wspierać replikację sesji pomiędzy klastrami serwerów aplikacyjnych (intra-cluster) poprzez sieci LAN/MAN/WAN |
| INF.AS.40. | Infrastruktura serwera aplikacji musi posiadać wbudowaną możliwość konfiguracji priorytetów obsługi żądań, priorytetów aplikacji i ich komponentów. Możliwość przypisywania reguł SLA do użytkowników, aplikacji i ich komponentów (np. servletów, EJB). Reguły SLA powinny obejmować takie cechy jak: wagi (priorytety – np. % czasu procesorów gwarantowany dla aplikacji i/lub ich komponentów), czasy odpowiedzi, min/max liczba wątków, itp. |
| INF.AS.41. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę pul połączeń do baz danych z uwierzytelnieniem połączeń. Tworzenie pul połączeń JDBC, w których jest możliwość zmapowania użytkowników serwera aplikacyjnego na użytkowników zdefiniowanych w bazie danych. Powinna być możliwość wykonania mapowania typu „user id per connection"; |
| INF.AS.42. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę wprowadzania zmian w kodzie Java w aplikacjach na serwerze bez konieczności re-deployment'u aplikacji ani restartu serwera aplikacyjnego (hot Java class swapping) |
| INF.AS.43. | Infrastruktura serwera aplikacji musi posiadać możliwość uruchamiania wielu działających równocześnie wersji tej samej aplikacji (ang. side-by-side deployment). Klienci, którzy rozpoczęli pracę z wcześniejszą wersją aplikacji powinni pracować z tą wersją aplikacji. Nowi klienci powinni pracować z nową wersją aplikacji. Serwer powinien zapewnić automatyczne wyłączanie poprzednich wersji aplikacji, w momencie, gdy ich użytkownicy zakończą pracę |
| INF.AS.44. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę integracji z technologią Microsoft COM. Możliwość wywoływania obiektów COM z poziomu aplikacji Java EE. Możliwość wywoływania kodu aplikacji Java EE z poziomu klientów COM. |
| INF.AS.45. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę Logging Last Resource - optymalizacji transakcji rozproszonych (XA) |
| INF.AS.46. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę zaawansowanych mechanizmów kolejkowych (JMS): grupowanie komunikatów przesyłanych do JMS z gwarancją zachowania kolejności ich przetworzenia (konsumpcji) wynikającą z kolejności ich utworzenia (produkcji) |
| INF.AS.47. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę zaawansowanych mechanizmów kolejkowych (JMS): możliwość łączenia komunikatów JMS w jednostki (grupy), a następnie przetwarzanie jednostek. Klient JMS nie może przetwarzać danej jednostki, dopóki w JMS nie pojawią się wszystkie komunikaty wchodzące w skład danej jednostki. Przetwarzanie różnych jednostek (niezależnych od siebie grup komunikatów) powinno być jednak możliwe. |
| INF.AS.48. | Infrastruktura serwera aplikacji musi posiadać wbudowany interfejs do JMS dla aplikacji napisanych w C (JMS C API) |
| INF.AS.49. | Infrastruktura serwera aplikacji musi posiadać wbudowany interfejs do JMS dla aplikacji napisanych w Microsoft .NET C# (JMS C# API) |
| INF.AS.50. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę zawieszania i wznawiania transakcji rozproszonych (XA) w ramach JTA API (suspend/resume) |

| | |
|---|---|
| INF.AS.51. | Infrastruktura serwera aplikacji musi posiadać wbudowany mechanizm współpracy z zewnętrznymi menedżerami transakcji rozproszonych (third-party, foreign transaction managers) |
| INF.AS.52. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę propagacji dodatkowych danych w ramach żądań (content propagation) |
| INF.AS.53. | Infrastruktura serwera aplikacji musi posiadać obsługę mechanizmu Store-and-Forward, czyli gwarantowanego, niezawodnego przesyłania komunikatów pomiędzy instancjami serwerów aplikacyjnych |
| INF.AS.54. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę asynchronicznych Web services (klient Web service, po wywołaniu Web service, nie musi zatrzymać się w oczekiwaniu na odpowiedź z Web service. Odpowiedź jest asynchronicznie przekazywana do klienta w późniejszym czasie) |
| INF.AS.55. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę Web services, które mogą wykonywać operacje na kliencie (callback Web service) |
| INF.AS.56. | Infrastruktura serwera aplikacji musi posiadać wbudowane wsparcie dla buforowanego wywoływania Web services |
| INF.AS.57. | Infrastruktura serwera aplikacji musi posiadać wbudowane wsparcie dla zewnętrznych dostawców usług kolejkowych (np. MQSeries) wraz z przenoszeniem kontekstów security i transakcyjnego |

Wymagania w zakresie współpracy z bazą danych uruchomioną w środowisku klastra bazodanowego:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AS.58. | Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę mechanizmu klastra bazodanowego – klastrowanie (failover/load balancing) na poziomie bazy danych, włącznie z poprawną obsługą transakcji rozproszonych w takim klastrowaniu |
| INF.AS.59. | Infrastruktura serwera aplikacji musi umożliwiać powiązanie sesji webowej użytkownika z konkretnym węzłem klastra bazodanowego |
| INF.AS.60. | Infrastruktura serwera aplikacji musi umożliwiać wykorzystanie usługi SCAN (Simple Client Access Name) dostępnej w bazie danych, która jest aktualnie funkcjonującym elementem środowiska Zamawiającego i będzie używana na potrzeby specyfikowanego środowiska |
| INF.AS.61. | Infrastruktura serwera aplikacji musi umożliwiać wykorzystanie mechanizmu powiązania wszystkich operacji w ramach globalnych transakcji z węzłem klastra na którym ta transakcja została zainicjowana. |
| INF.AS.62. | Infrastruktura serwera aplikacji musi umożliwiać aktywne wykorzystanie informacji o stanie klastra bazodanowego, w szczególności o niedostępności poszczególnych węzłów klastra bazodanowego lub o pojawieniu się nowych węzłów. |
| INF.AS.63. | Infrastruktura serwera aplikacji musi umożliwiać aktywne wykorzystanie informacji o aktualnym obciążeniu poszczególnych węzłów klastra bazodanowego |
| INF.AS.64. | Infrastruktura serwera aplikacji musi być certyfikowana dla współpracy ze środowiskiem bazodanowym Zamawiającego. Certyfikat musi być wystawiony przez producenta bazy danych. |

Wymagania w zakresie mechanizmów administracji, zarządzania oraz monitorowania:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AS.65. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać zarządzanie i monitorowanie wieloma serwerami aplikacyjnymi z jednej konsoli |
| INF.AS.66. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać zarządzanie i monitorowanie wielu aplikacji wdrożonych na różnych instancjach serwera aplikacyjnego |
| INF.AS.67. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać zarządzanie klastrami serwerów aplikacyjnych |
| INF.AS.68. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać monitorowanie zasobów serwerów aplikacyjnych takich jak póle połączeń JDBC, kolejki JMS, źródła danych |
| INF.AS.69. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać monitorowanie w czasie rzeczywistym zdarzeń płynących z wielu serwerów aplikacyjnych z możliwością |

| | |
|---|---|
| | wyspecyfikowania:<br>- Poziomów zdarzeń krytycznych oraz ostrzeżeń<br>- Różnych metod notyfikacji o zdarzeniach<br>- Definiowanie reguł notyfikacyjnych<br>- Możliwości podpięcia akcji naprawczych pod zdarzenie |
| INF.AS.70. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać centralne zarządzanie incydentami i problemami |
| INF.AS.71. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać raportowanie wydajności systemów z możliwością:<br>- Wyspecyfikowania zakresu czasowego wyświetlanych danych<br>- Wyświetlania danych z różnych komponentów na jednym raporcie (wykresie)<br>- Zapisania aktualnych danych wydajnościowych jako wzorca do porównywania z przyszłymi danymi |
| INF.AS.72. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać dostęp do logów zarządzanych serwerów aplikacyjnych z możliwością:<br>- Filtrowania po czasie wpisu do logów<br>- Filtrowania poziomie zalogowanej informacji (error, warning, etc.)<br>- Pobrania pliku logu lub wyeksportowania wiadomości do pliku |
| INF.AS.73. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać możliwości monitorowania poziomu dostępności usługi (SLA) względem zdefiniowanych parametrów (mierników) |
| INF.AS.74. | Moduł Zarządzania infrastruktury serwera aplikacji musi umożliwiać monitorowanie i diagnostyka JVM:<br>- Bez konieczności wprowadzania specyficznych zmian w kodzie aplikacji<br>- Bez konieczności restartu serwera<br>- Pełny wgląd w dane maszyny wirtualnej Java (wątki, stos, etc)<br>- Analiza wpływu działania maszyny wirtualnej Java na bazę danych i odwrotnie. |
| INF.AS.75. | Infrastruktura serwera aplikacji musi posiadać wbudowaną możliwość konfiguracji ochrony serwerów aplikacyjnych (i aplikacji) przed przeciążeniem. Dla przykładu: jeśli liczba żądań do serwera/aplikacji jest zbyt duża, serwer powinien przekierować nowe żądania do innych instancji w klastrze |
| INF.AS.76. | Infrastruktura serwera aplikacji musi umożliwiać automatyczny restart serwera i/lub aplikacji w sytuacji ich zawieszenia (braku odpowiedzi), pojawienia się błędów o braku pamięci lub zbyt długiego wykonywania się wątków (stuck threads) |
| INF.AS.77. | Infrastruktura serwera aplikacji musi posiadać możliwość ograniczenia liczby sesji HTTP w serwerze tworzonych przez daną aplikację |
| INF.AS.78. | Infrastruktura serwera aplikacji musi posiadać możliwość rozdziału ruchu (protokołów) na różne interfejsy sieciowe (lub adresy IP). Np. możliwość rozdzielenia ruchu administracyjny/monitoringu od ruchu aplikacyjnego do ruchu związanego z funkcjonowaniem klastra (replikacja sesji) – dane związane z tymi funkcjami mogą być przesyłane poprzez inne karty sieciowe/podsieci, itp. |
| INF.AS.79. | Infrastruktura serwera aplikacji musi posiadać możliwość automatycznego i ręcznego restartu (migracji) instancji serwerów aplikacyjnych na innych fizycznych maszynach w razie awarii, wraz z przeniesieniem istotnych dla przetwarzania danych (np. zawartość kolejek JMS, logi transakcji rozproszonych JTA). Automatyczna rekonfiguracja serwerów aplikacyjnych po restarcie (zmiana adresu IP, itp.) |
| INF.AS.80. | Infrastruktura serwera aplikacji musi posiadać możliwość konfiguracji i zarządzania środowiskiem serwerów aplikacyjnych równocześnie poprzez: konsole webowe, skrypty (np. Jython), programowo (Java API), SNMP |
| INF.AS.81. | Infrastruktura serwera aplikacji musi posiadać możliwość łatwego rozszerzania funkcjonalności oferowanych przez konsole administracyjne. Rozszerzenia nie powinny wymagać zmian w kodzie istniejących konsol. Rozszerzenia nie powinny wymagać zmian w przypadku przyszłych aktualizacji (upgrade wersji serwera aplikacyjnego, itp.) |
| INF.AS.82. | Infrastruktura serwera aplikacji musi posiadać możliwość wprowadzania zmian w konfiguracji środowiska serwerów aplikacyjnych w sposób transakcyjny (albo wszystkie zmiany zostaną poprawnie wprowadzone albo żadna zmiana nie będzie wprowadzona) |

| | |
|---|---|
| INF.AS.83. | Infrastruktura serwera aplikacji musi posiadać możliwość automatycznego tworzenia skryptów konfiguracyjnych (rejestrowanie wykonywanych zmian, a następnie ich zapisywanie do pliku, tak, aby później taki plik uruchomić w postaci skryptu) |
| INF.AS.84. | Infrastruktura serwera aplikacji musi posiadać wbudowany mechanizm automatycznej naprawy transakcji (transaction recovery) podczas restartu serwera aplikacyjnego |
| INF.AS.85. | Infrastruktura serwera aplikacji musi posiadać wbudowany moduł do diagnostyki pracy serwera aplikacyjnego i uruchomionych w nim aplikacji. Możliwość dynamicznego dodawania poprzez konfigurację własnego kodu diagnostycznego do określonych miejsc w aplikacji i jej komponentach |
| INF.AS.86. | Infrastruktura serwera aplikacji musi posiadać możliwość zarządzania i monitorowania wieloma serwerami aplikacyjnymi z jednej konsoli |
| INF.AS.87. | Infrastruktura serwera aplikacji musi posiadać możliwość zarządzania i monitorowania wielu aplikacji wdrożonych na różnych instancjach serwera aplikacyjnego |
| INF.AS.88. | Infrastruktura serwera aplikacji musi posiadać możliwość zarządzania klastrami serwerów aplikacyjnych |
| INF.AS.89. | Infrastruktura serwera aplikacji musi posiadać możliwość monitorowania zasobów serwerów aplikacyjnych takich jak póle połączeń JDBC, kolejki JMS, źródła danych |

### 5.6.3 Infrastruktura cache

Oferowana infrastruktura cache dostarczana wraz z serwerem aplikacji musi minimalnie spełniać następujące wymagania:

| ID wymagania | Opis wymagania |
|---|---|
| INF.CACHE.1. | Wsparcie podstawowych technologii programistycznych (API pozwalające implementować komunikację aplikacji z infrastrukturą cache)., w tym:<br>• Java,<br>• Technologia .NET<br>• C/C++. |
| INF.CACHE.2. | Infrastruktura cache musi umożliwiać realizację integracji aplikacji z infrastrukturą cache poprzez usługi typu REST |
| INF.CACHE.3. | Wsparcie funkcjonalności związanej z przechowywaniem sesji (persystencja sesji http, kontekstu usług typu Servlet oraz kontekstu usług typu Session EJB) dla zaproponowanego serwera aplikacji |
| INF.CACHE.4. | Możliwość rozproszonego przetwarzania danych w pamięci cache. Oznacza to, że operacje na danych związane z przetwarzaniem odbywają się bezpośrednio w pamięci cache, bez konieczności transportu danych poza obręb pamięci cache. |
| INF.CACHE.5. | Możliwość przechowywania obiektów w strukturze kolekcji (Klucz, Wartość) |
| INF.CACHE.6. | Wsparcie modelu obiektowego przechowywanych danych |
| INF.CACHE.7. | Oprogramowanie infrastruktury cache musi zapewniać mechanizm rozproszonej pamięci operacyjnej (ang. Single System Image) |
| INF.CACHE.8. | Możliwość śledzenia zmian w danych znajdujących się w pamięci cache |
| INF.CACHE.9. | Możliwość równoległego wyszukiwania danych oraz możliwość tworzenia indeksów |
| INF.CACHE.10. | Oprogramowanie infrastruktury cache musi zapewniać funkcjonalność zapytań ciągłych, co oznacza możliwość otrzymywania zawsze aktualnych wyników wyszukiwania. |
| INF.CACHE.11. | Możliwość rozproszonego (równoległego) agregowania danych w oparciu o filtry. Minimalnie muszą występować filtry (MINIMUM, MAXIMUM, AVERAGE, SUM, HAVING, GROUP BY, DISTINCT). |
| INF.CACHE.12. | Możliwość stosowania / budowania własnych funkcji agregujących. |
| INF.CACHE.13. | Oprogramowanie infrastruktury cache musi zapewniać mechanizmy wysokiej dostępności i ochrony danych przed awariami |
| INF.CACHE.14. | Możliwość klastrowania węzłów cache |
| INF.CACHE.15. | Oprogramowanie infrastruktury cache musi zapewniać płynne dodawanie i usuwanie węzłów klastra cache |
| INF.CACHE.16. | Oprogramowanie infrastruktury cache musi zapewniać przezroczystą obsługa awarii |

| | |
|---|---|
| | pojedynczych węzłów. |
| INF.CACHE.17. | Oprogramowanie infrastruktury cache mimo występowania w konfiguracji wielowęzłowej przechowującej dane, nie może wymagać wspólnej przestrzeni (np. bazy danych, rejestru, itd.) |
| INF.CACHE.18. | Oprogramowanie infrastruktury cache musi zapewniać mechanizm cache, pomiędzy aplikacją a drugą aplikacją lub bazą danych |
| INF.CACHE.19. | Oprogramowanie infrastruktury cache musi zapewniać persystencję przechowywanych danych w bazie danych |
| INF.CACHE.20. | Możliwość budowania własnych mechanizmów integrujących cache z dowolnymi repozytoriami danych (bazy danych, katalogi, własne aplikacje udostępniające dane poprzez API) |
| INF.CACHE.21. | Oprogramowanie infrastruktury cache musi zapewniać mechanizm read through w komunikacji na linii aplikacja <-> cache <-> baza danych |
| INF.CACHE.22. | Oprogramowanie infrastruktury cache musi zapewniać mechanizm write through w komunikacji na linii aplikacja <-> cache <-> baza danych |
| INF.CACHE.23. | Oprogramowanie infrastruktury cache musi zapewniać mechanizm write behind w komunikacji na linii aplikacja <-> cache <-> baza danych |
| INF.CACHE.24. | Mechanizm write behind musi zapewniać możliwość kolejkowania zapisów do bazy danych |
| INF.CACHE.25. | Mechanizm kolejkowania żądań związanych z bazą danych musi być odporny na awarie (musi być automatycznie tworzona kopia zapasowa kolejek) |
| INF.CACHE.26. | Możliwość rozszerzenia cache do pracy w sieci WAN (odporność na mniejsze przepustowości oraz większe opóźnienia) |
| INF.CACHE.27. | Możliwość integracji z technologią Spring |
| INF.CACHE.28. | Możliwość integracji z technologią Hibernate |
| INF.CACHE.29. | Oprogramowanie infrastruktury cache musi zapewniać mechanizm wyzwalaczy (ang. triggers) |
| INF.CACHE.30. | Możliwość usuwania z pamięci kopii danych po zapisaniu ich do persystentnego repozytorium danych (np. bazy danych) |

### 5.6.4 Oprogramowanie antywirusowe

Oprogramowanie umożliwiające wykonywanie usług antywirusowych dla serwerów fizycznych oraz wirtualnych w zamawianej Platformie oraz środowiskach klienckich.

W zakresie ochrony serwerów fizycznych i wirtualnych system musi spełniać minimum następujące rozwiązania:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AVS.1. | System musi zapewniać bezpieczeństwo fizycznych i wirtualnych serwerów oraz stacji użytkowników końcowych. |
| INF.AVS.2. | System musi pozwalać na wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych, oraz zwirtualizowanych desktopów. |
| INF.AVS.3. | System powinien zawierać zaawansowane funkcje zarządzania, upraszczające zakres zadań ochrony. |
| INF.AVS.4. | Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa. |
| INF.AVS.5. | System musi mieć możliwość konfiguracji rozwiązania, które będzie dla wyznaczonych agentów punktem dystrybuującym uaktualnienia i poprawki oprogramowania. |
| INF.AVS.6. | System musi wykorzystywać VMware vShield API do zapewnienia bezpieczeństwa chronionych systemów w przypadku systemów uruchomionych na platformie VMware. |
| INF.AVS.7. | System musi umożliwiać zdefiniowanie harmonogramu lub częstotliwości pobierania aktualizacji wirusów od producenta systemu. |
| INF.AVS.8. | System musi wykorzystywać mechanizmy cache i deduplikacji w celu optymalizacji czasu skanowania i wykrywania zmian. |

| | |
|---|---|
| INF.AVS.9. | System musi umożliwiać instalację i konfigurację lokalnego serwera skorelowanej reputacji plików, synchronizującego się z chmurą producenta, który pozwalał będzie na weryfikację reputacji plików bez konieczności łączenia się z Internetem |
| INF.AVS.10. | System musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa. |
| INF.AVS.11. | System musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, itd. |
| INF.AVS.12. | System musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów. |
| INF.AVS.13. | System musi pozwalać na zarządzanie zdarzeniami i natychmiastowe alarmowanie i raportowanie o aktywności wirusów w chronionej infrastrukturze na kilka sposobów |
| INF.AVS.14. | Zarządzanie systemem musi odbywać się poprzez standardową przeglądarkę WWW i połączenie https, która nie wymaga instalacji żadnych dodatkowych komponentów. |
| INF.AVS.15. | System musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP lub wywołania komendy. |
| INF.AVS.16. | System musi umożliwiać tworzenie administratorów o różnych stopniach uprawnień w stosunku do różnych modułów i funkcjonalności systemu, a także w stosunku do różnych chronionych obiektów lub grup obiektów. |
| INF.AVS.17. | Zarządzanie rolami w systemie musi pozwalać zdefiniowanie uprawnień dających możliwość administrowania wyłącznie jednym chronionym obiektem oraz pojedynczymi funkcjonalnościami systemu bez możliwości zmiany nadrzędnego profilu bezpieczeństwa |
| INF.AVS.18. | System musi pozwalać na tworzenie struktur zarządzanych komputerów również poprzez adresacje IP komputera który podlega zarządzaniu. |
| INF.AVS.19. | System musi być przygotowany do pracy w strefie DMZ tak aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną. |
| INF.AVS.20. | System musi prezentować dane w formie graficznej w panelu głównym |
| INF.AVS.21. | System musi umożliwiać na jednoczesny dostęp do konsoli zarządzającej niezależnie przez kilku administratorów. |
| INF.AVS.22. | System musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. |
| INF.AVS.23. | System nie może wymagać restartu chronionych komputerów i serwerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. |
| INF.AVS.24. | System musi pozwalać na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan". |
| INF.AVS.25. | System musi pozwalać na automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa. |
| INF.AVS.26. | System musi zapewniać w procesie skanowania ręcznego i automatycznego przeskanowania dowolnego celu pod względem złośliwego oprogramowania |
| INF.AVS.27. | System musi umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu systemu i chronionych obiektów. |
| INF.AVS.28. | System musi umożliwiać tworzenie dowolnej ilości profilów bezpieczeństwa zawierających predefiniowane reguły ochronne. |
| INF.AVS.29. | System musi umożliwiać generowanie na żądanie oraz wg harmonogramu raportów w formatach minimalnie RTF oraz PDF oraz możliwość zabezpieczenie raportu poprzez jego zaszyfrowanie lub zabezpieczenie hasłem. |
| INF.AVS.30. | System musi współpracować co najmniej z bazami danych Oracle, Microsoft SQL oraz DB2 |
| INF.AVS.31. | System musi pozwalać na bezagentową ochronę środowisk wirtualnych opartych o platformę VMware vSphere w wersjach 4.x oraz 5.x |

W zakresie ochrony farmy serwerów wirtualnych system musi spełniać minimum następujące wymagania:

| ID wymagania | Opis wymagania |
|---|---|
| INF.AVS.32. | System musi pozwalać na monitorowanie integralności chronionych systemów poprzez wykrywanie zmian w zdefiniowanych zasobach (wskazane katalogi i elementy rejestru systemu) |

| | |
|---|---|
| INF.AVS.33. | System musi posiadać możliwość skanowania i wykrywania zmian w strukturze chronionych obiektów. |
| INF.AVS.34. | System musi posiadać możliwość zdefiniowania własnych reguł wykrywających zmiany z zdefiniowanych fragmentach rejestrów systemowych Windows. |
| INF.AVS.35. | System musi posiadać możliwość zdefiniowania własnych reguł wykrywających zmiany z zdefiniowanych folderach. |
| INF.AVS.36. | System musi posiadać możliwość zdefiniowania wykluczeń plików znajdujących się w obszarze objętych ochroną integralności. |
| INF.AVS.37. | System musi posiadać predefiniowane reguły chroniące krytyczne elementy chronionych systemów informatycznych. |
| INF.AVS.38. | System musi pozwalać na śledzenie i korelację zdarzeń występujących na chronionych obiektach ze zdefiniowanych dzienników lub plików typu log. |
| INF.AVS.39. | System musi umożliwiać analizowanie logów z programów zainstalowanych na chronionych systemach informatycznych. |
| INF.AVS.40. | System musi umożliwiać analizowania logów ze zdefiniowanych plików znajdujących się na chronionych systemach informatycznych. |
| INF.AVS.41. | System musi umożliwiać analizowanie niestandardowych formatów plików typu log. |
| INF.AVS.42. | System musi posiadać możliwość kontroli oraz blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną. |
| INF.AVS.43. | System musi posiadać predefiniowaną bazę najpopularniejszych aplikacji oraz komunikatorów (włączając w to gadu-gadu) |
| INF.AVS.44. | System musi posiadać możliwość heurystycznego wykrywania transmisji na podstawie częstotliwości jej występowania oraz zdefiniowanego zakresu portów. |
| INF.AVS.45. | System musi posiadać możliwość wykrywania ataków typu SQL injection oraz cross-site-scripting wraz z możliwością ustanowienia progów alarmu jak i dodawania i edytowania nowych ciągów danych. |
| INF.AVS.46. | System musi posiadać możliwość przełączania pomiędzy trybem blokowania ruchu i trybem detekcji zdarzeń w sposób globalny dla wszystkich reguł. |
| INF.AVS.47. | System musi posiadać moduł umożliwiający blokowanie transmisji na podstawie zdefiniowanej charakterystyki ruchu na podstawie sygnatury oraz zdefiniowanego ciągu znaków (patternu). Funckjonalność ta powinna być dostarczana zarówno w ramach agenta zainstalowanego na chronionym obiekcie jak i bezagentowo w przypadku środowisk wirtualnych VMware. |
| INF.AVS.48. | System musi pozwalać na sprawdzanie w czasie rzeczywistym poziomu bezpieczeństwa nieznanych aplikacji poprzez zapytania przesyłane poprzez siec do systemu serwerów producenta. |
| INF.AVS.49. | System musi posiadać pełnostanowy firewall (stateful firewall) pozwalający na łatwą izolacje interfejsów i nie wymagający restartów systemu. Funckjonalność ta powinna być dostarczana zarówno w ramach agenta zainstalowanego na chronionym obiekcie jak i bezagentowo w przypadku środowisk wirtualnych VMware. |
| INF.AVS.50. | System musi pełni wspierać IPv6 |
| INF.AVS.51. | System musi umożliwiać kontrolę połączeń wychodzących i przychodzących w komunikacji sieciowej z możliwością kontroli niestandardowych portów TCP (możliwość zdefiniowania na podstawie numeru protokołu oraz numeru typu ramki). Funckjonalność ta powinna być dostarczana zarówno w ramach agenta zainstalowanego na chronionym obiekcie jak i bezagentowo w przypadku środowisk wirtualnych VMware. |
| INF.AVS.52. | System musi posiadać możliwość przełączenia trybu działania reguł firewalla z trybu blokowania ruchu w tryb detekcji zdarzeń |

### 5.6.5 Oprogramowanie do backupu i archiwizacji

Oprogramowanie umożliwiające wykonywanie usług backupu i archiwizacji w Platformie z wykorzystaniem zamawianej infrastruktury macierzowej.

Wymagania minimalne:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BACK.1. | Obsługa urządzeń taśmowych i dyskowych do przechowywania kopii zapasowych i archiwizacji danych. |
| INF.BACK.2. | Przechowywanie konfiguracji polityk zabezpieczeń oraz informacji o wykonanych kopiach, harmonogramach oraz nośnikach w relacyjnej bazie danych. Proces tworzenia kopii zapasowej oraz odtwarzania danych powinien być procesem transakcyjnym. Ze względów bezpieczeństwa system powinien mieć możliwość wykonania mirroring'u tej bazy danych, przynamniej na poziomie logów transakcyjnych. Jednocześnie musi istnieć możliwość wykonani kopii zapasowej na taśmy w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności. |
| INF.BACK.3. | System backupu musi w sposób automatyczny i bezobsługowy optymalizować parametry pracy swojej bazy danych. |
| INF.BACK.4. | Możliwość definiowania w sposób centralny polityki tworzenia kopii zapasowych, tj. określenia, jakie dane, kiedy i gdzie powinny być składowane (definiowanie harmonogramu backup'u). |
| INF.BACK.5. | Możliwość realizowanie raz zdefiniowanej polityki backupu w sposób automatyczny, bez konieczności ingerencji operatora. System powinien umożliwić także wykonywanie określonej akcji (uruchomienie polecenia lub skryptu) na zabezpieczanym systemie, przed i po zadaniu backupowym (np. zatrzymanie procesów, wykonanie backupu i ponowne uruchomienie). |
| INF.BACK.6. | Wykonywanie kopii zapasowych w sposób przyrostowy – pierwsza kopia powinna być kopią całkowitą a kolejne powinny zawierać jedynie dane, które uległy modyfikacji. |
| INF.BACK.7. | Możliwość zdefiniowania czasu ważności kopii danych, tj. czasu po którym kopie te zostaną automatycznie usunięte. |
| INF.BACK.8. | Możliwość jednoczesnego tworzenia kopii zapasowych na różnego rodzaju nośniki (taśmy, dyski). |
| INF.BACK.9. | Możliwość definiowanie maksymalnej ilości wersji zabezpieczanych plików. W razie przekroczenia limitu z repozytorium powinny być usuwane wersje najstarsze. |
| INF.BACK.10. | Możliwość jednoczesnego tworzenia kopii zapasowych z wielu klientów (zasobów) na urządzenia dyskowe. System bez ingerencji operatora powinien przenieść dane z dysków na taśmy w przypadku osiągnięcia zdefiniowanego poziomu wypełnienia przestrzeni dyskowej serwera kopii zapasowych. |
| INF.BACK.11. | Możliwość tworzenie kopii zapasowych tzw. On-linie z serwera pocztowego MS Exchange, bez konieczności zatrzymywania pracy serwera |
| INF.BACK.12. | Możliwość tworzenie kopii zapasowych tzw. on-line z serwerów baz i aplikacji MSSQL, Oracle, SAP, MS SharePiont, DB2, Informix, bez konieczności zatrzymywania pracy serwera bazy danych |
| INF.BACK.13. | Możliwość ciągłego zabezpieczenia danych ze stacji roboczych (tworzenia kopii zapasowej w momencie modyfikacji pliku). |
| INF.BACK.14. | Automatyczne optymalizowanie położenia danych na taśmach pod kątem wykorzystania nośników: system powinien zapewniać średnie wykorzystanie taśm magnetycznych dostępnych do przechowywania danych na poziomie min 70%. |
| INF.BACK.15. | Automatyczne defragmentowanie danych na taśmach. |
| INF.BACK.16. | Możliwość włączenia automatycznego mechanizmu minimalizującego rozproszenie danych pochodzących z określonego zasobu na nośnikach; możliwość stosowania tego mechanizmów dla następujących klas zasobów:<br>- system plików wolumin dyskowy,<br>- host (klient systemu kopii zapasowych),<br>- grupa hostów.<br>Funkcja ta powinna gwarantować minimalną ilość niezbędnych operacji montowania nośnika przy odzyskiwaniu danych z określonego zasobu. |
| INF.BACK.17. | Możliwość utworzenia dodatkowego obszaru składowania danych na wybranym urządzeniu (systemie dyskowym, bibliotece taśmowej lub wirtualnej bibliotece taśmowej - VTL), zawierającego wyłącznie aktualne (lub najnowsze) wersje istniejących plików na zabezpieczanych systemach. Proces uaktualniania tego dodatkowego składowiska kopii powinien odbywać się automatycznie, bez konieczności komunikacji pomiędzy serwerem backupów i systemem zabezpieczanym (korzystając z danych już zeskładowanych w systemie kopii zapasowych). W przypadku przechowywania danych na taśmach system powinien |

| | |
|---|---|
| | umożliwiać przeprowadzenie tego procesu bez konieczności wykorzystania (tymczasowego lub stałego) przestrzeni dyskowej. |
| INF.BACK.18. | Tworzenie dodatkowych instancji kopii w celu zabezpieczenia przed uszkodzeniem urządzenia dyskowego lub nośnika magnetycznego używanego do przechowywania kopii zapasowych. |
| INF.BACK.19. | System powinien umożliwiać wykorzystanie dodatkowych kopii do składowania off-site (poza lokalizacją chronionych systemów) i zarządzać rotacją nośników używanych w tym procesie. |
| INF.BACK.20. | Zarządzanie politykami retencji na poziomie grup systemów, pojedynczych systemów, systemów plików/woluminów dyskowych, katalogów, pojedynczych plików i obiektów, wzorców nazw plików i ścieżek dyskowych. |
| INF.BACK.21. | Możliwość odzyskania danych dostępnych na chronionym systemie w określonym punkcie w czasie (w zakresie polityki retencji). |
| INF.BACK.22. | Możliwość wznowienia przerwanego zadania odtwarzania z pominięciem już odtworzonych danych. |
| INF.BACK.23. | System oprócz backupu i odtwarzania danych musi realizować funkcje archiwizacji danych – tworzenia kopii przechowywanej przez określony czas niezależnie od zmian na systemie chronionym, z możliwością przeniesienia danych do systemu kopii zapasowych (skasowania danych na systemie chronionym po utworzeniu ich kopii archiwalnej w systemie kopii zapasowych). |
| INF.BACK.24. | Odtwarzanie danych na inny niż źródłowy system, katalog lub z nową nazwą pliku. |
| INF.BACK.25. | Tworzenie i odtwarzanie kopii zapasowych z wykorzystaniem SAN (Storage Area Network) – dane będą przesyłane do i z- serwera kopii zapasowych bez obciążania LAN (sieci TCP/IP). |
| INF.BACK.26. | Możliwość integracji z mechanizmami sprzętowego szyfrowania nośników taśmowych |
| INF.BACK.27. | Możliwość nieodwracalnego usunięcia kopii danych z systemu przez zamazanie nośników magnetycznych. |
| INF.BACK.28. | Możliwość komunikacji z klientem systemu kopii zapasowych za pomocą protokołu SSL. |
| INF.BACK.29. | Możliwość jednoczesnego zapisu i odczytu danych z dyskowych urządzeń składowania. |
| INF.BACK.30. | Możliwość odtworzenia pojedynczego obiektu z Microsoft Active Directory bez restartu serwera |
| INF.BACK.31. | Możliwość minimalizacji redundancji danych przesyłanych z klientów systemu kopii zapasowych (tzw. deduplikacja danych na systemie źródłowym) – mechanizm musi być wbudowany w oprogramowanie |
| INF.BACK.32. | Możliwość automatycznej minimalizacji redundancji danych składowanych po stronie serwera (tzw. deduplikacja danych na systemie docelowym) – mechanizm musi być wbudowany w oprogramowanie |
| INF.BACK.33. | Monitorowanie i raportowanie o zadaniach (harmonogramach) oraz o wykorzystaniu zasobów systemowych i zarządzanych pamięci masowych. |
| INF.BACK.34. | Możliwość definiowania kryteriów alarmów na podstawie dowolnych danych systemu backupu. |
| INF.BACK.35. | Możliwość integracji z VCB (VMware Consolidated Backup), vStorage API oraz możliwość odtworzenia wirtualnych maszyn z poziomu klienta systemu backupu. |
| INF.BACK.36. | Możliwość integracji z technologią CBT (changed block trakcing) środowiska vSphere oraz VMware ESX. |
| INF.BACK.37. | Możliwość wykonywania kopii zapasowej danych zgromadzonych na serwerze kopii zapasowych i możliwość odtworzenia z nich kompletnego środowiska w przypadku awarii serwera. |
| INF.BACK.38. | Możliwość wykorzystania wielu strumieni zapisu podczas procesu tworzenia kopii zapasowej bazy danych serwera kopii zapasowych w celu przyśpieszenia wykonywania kopii |
| INF.BACK.39. | Możliwość sprawdzania poprawności danych podczas procesu zapisu/odczytu z urządzeń taśmowych |
| INF.BACK.40. | Możliwość automatycznego wykonywania uaktualnienia oprogramowania klienta backupu i zarządzania tym procesem z centralnej konsoli |
| INF.BACK.41. | Możliwość replikacji danych (zapasowych kopii oraz informacji o klientach) na drugi serwer kopii zapasowych. |
| INF.BACK.42. | Możliwość zapisu danych podczas wykonywania kopii zapasowej na co najmniej 2 urządzenia (dwa obszary składowania danych). |
| INF.BACK.43. | Wymagania dotyczące licencji: Dostarczone licencje muszą umożliwiać obsługę co najmniej 64 slotów w bibliotece taśmowej |

Konfiguracja oferowanej platformy kopii zapasowych i przechowywania danych musi uwzględniać wykonanie następujących czynności:

| ID wymagania | Opis wymagania |
|---|---|
| INF.BACK.44. | Utworzenie grup dyskowych i implementacja RAID wg ustaleń z Zamawiającym |
| INF.BACK.45. | Utworzenie LUN-ów oraz ich prezentacja serwerom platformy wirtualizacyjnej oraz serwerowi zarządzającemu. |
| INF.BACK.46. | Opracowanie polityki backupu oraz testów odtworzeniowych. |
| INF.BACK.47. | Instalacja składników oprogramowania systemu backupu i replikacji. |
| INF.BACK.48. | Konfiguracja backupu maszyn wirtualnych w układzie DiskToDiskToTape z deduplikacją wg. ustalonego ze Zleceniodawcą harmonogramu i opracowanej polityki backupu. Testy odtworzeniowe maszyn wirtualnych, pojedynczych plików systemów operacyjnych oraz pojedynczych obiektów aplikacji. |
| INF.BACK.49. | Konfiguracja bezpośrednich (z poziomu systemu operacyjnego) backupów wskazanych przez Zleceniodawcę plików na napędy taśmowe, wraz z testami odtworzeniowymi. |
| INF.BACK.50. | Konfiguracja cyklicznych replikacji wskazanych przez Zamawiającego maszyn wirtualnych pomiędzy macierzami dyskowymi. Testy uruchomieniowe maszyn wirtualnych z repliki. |

## 5.7 Infrastruktura integracji i budowania usług złożonych

Świadczenie usług w modelu PaaS, FaaS oraz SaaS stawia przed Data Techno Park znaczne wymagania w zakresie integracji zamawianych aplikacji.

Integracja aplikacji następować będzie w oparciu o jawne definicje procesów osadzonych w silniku procesów stanowiącym element szyny integracyjnej.

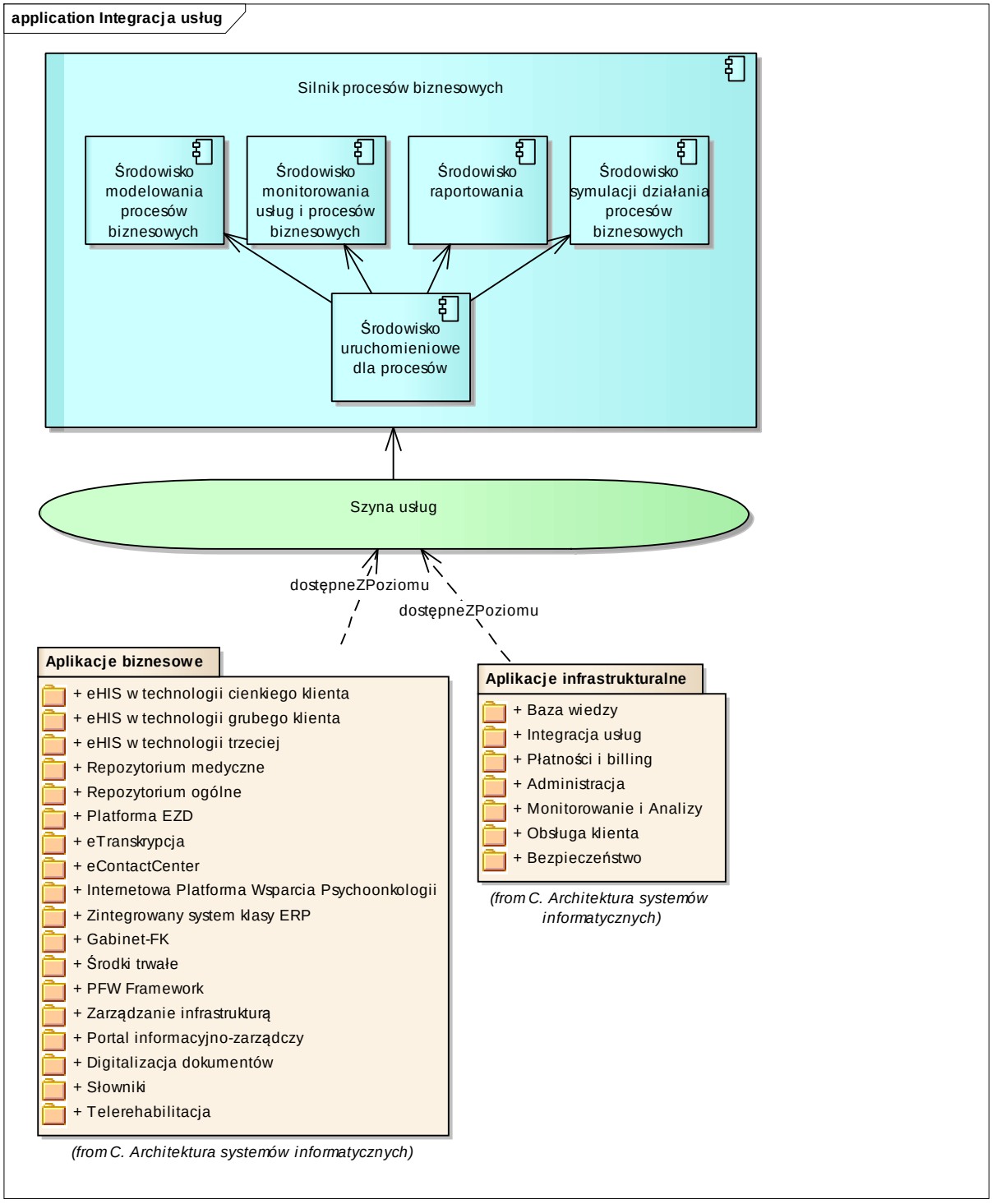
Każda aplikacja, której model zakłada istnienie interfejsów w postaci API musi być dostępna z poziomu szyny usług. Oznacza to, że usługi muszą być publikowane w rejestrze szyny usług, w jednym z dozwolonych modeli.

Przewiduje się logiczne wydzielenie 2 typów szyn integracyjnej: jednej dla komunikacji pomiędzy aplikacjami wewnątrz infrastruktury Data Techno Park oraz jednej dla komunikacji z siecią WAN (zewnętrznej). Zewnętrzna szyna może być dedykowanym rozwiązaniem aplikacyjnym zapewniającym skuteczną filtrację ruchu z zewnątrz i gwarantującym bezpieczeństwo zasobów dostępnych z poziomu wewnętrznej szyny usług.

Wewnętrzna szyna usług będzie podstawową szyną usług, na której osadzone muszą być wszystkie usługi aplikacyjne, zarówno biznesowe, jak i infrastrukturalne.

W skład infrastruktury do integracji i budowania usług złożonych wchodzą następujące klasy oprogramowania:

1. Szyna usługowa (ang. Enterprise Service Bus, ESB)
2. Silnik procesów biznesowych (ang. Business Process Modelling, BPM) składający się z:
    a. środowiska uruchomieniowego dla procesów biznesowych
    b. środowiska modelowania procesów biznesowych
    c. środowiska monitorowania usług i procesów biznesowych
    d. środowiska symulacji działania procesów biznesowych
    e. środowiska raportowania




Rysunek 10 Integracja usług i rola wewnętrznej szyny usług

Wszystkie typy oprogramowania muszą być ze sobą silnie zintegrowane oraz dostarczone w postaci gotowego oprogramowania jako jeden spójny produkt wykonany przez jednego dostawcę.

### 5.7.1 Szyna usługowa

| ID wymagania | Opis wymagania |
|---|---|
| ESB.1. | Oprogramowanie Szyny Usług będzie oparte o serwer aplikacji zgodny ze standardem JEE (Java |

| | |
|---|---|
| | Enterprise Edition). |
| ESB.2. | Oprogramowanie musi być dostarczone z licencjami umożliwiającymi jego uruchomienie na infrastrukturze określonej w zestawieniu ilościowym, przy czym zakłada się, że liczba licencji nie będzie wystarczająca do obsadzenia całości serwera, dlatego dopuszcza się zastosowanie wirtualizacji umożliwiającej pracę oprogramowania w liczbie zakładanej z zestawieniu ilościowym. |
| ESB.3. | Oprogramowanie będzie umożliwiało integrację w oparciu o standardy EJB 3.0 oraz Spring Framework. |
| ESB.4. | Oprogramowanie będzie zgodne ze standardami:<br>a. WSDL 2.0<br>b. SOAP 1.2<br>c. SOAP with Attachments<br>d. UDDI 3.0 |
| ESB.5. | Oprogramowanie umożliwi projektowanie bezstanowych procesów biznesowych z pominięciem warstwy Zarządzania Procesami Biznesowymi. |
| ESB.6. | Oprogramowanie umożliwi realizację bezstanowych ale długotrwałych procesów zależnych od wielu usług – agregacja usług. |
| ESB.7. | Oprogramowanie umożliwi implementację usług przekazywania zadań do innych usług wraz z translacją komunikatów. |
| ESB.8. | Oprogramowanie umożliwi zdefiniowanie reguł wywołania usługi. |
| ESB.9. | Oprogramowanie umożliwi ograniczenie wywołań usług, ochronę wydajności adapterów oraz zajętości kolejek. |
| ESB.10. | Oprogramowanie umożliwi implementację komunikacji bezpośredniej aplikacjami biznesowymi i infrastrukturalnymi na podstawie posiadanych adapterów. |
| ESB.11. | Oprogramowani umożliwi transformację danych, transformację komunikatów np. XPath/XSLT/XQuery. |
| ESB.12. | Oprogramowanie umożliwi wzbogacanie transformacji danych o warunki logiczne lub ograniczenia. |
| ESB.13. | Oprogramowanie będzie wspierało transformację danych poza strukturą XML np. plików tekstowych. |
| ESB.14. | Oprogramowanie będzie obsługiwało wiele warstw transportowych np.: JMS, HTTP, MQ, FTP, TCP. |
| ESB.15. | Oprogramowanie umożliwi monitorowanie poprawnej pracy usług. |
| ESB.16. | Wraz z oprogramowaniem zostaną dostarczone niezbędne skrypty oraz narzędzia wspierające przełączanie aktywności pomiędzy węzłami Szyny Usług. |
| ESB.17. | Oprogramowanie zapewni wsparcie w zakresie realizacji testów wydajnościowych i funkcjonalnych: zaślepki, symulatory, skrypty automatyzujące testy, konsola wywoływania ręcznego usług. |
| ESB.18. | Oprogramowanie będzie wspierało transformację komunikatów, na podstawie przykładowej wymiany plików XML przekazywanych transportem FTP i na podstawie zawartych w nim danych wywoływanie odpowiednich usług. |
| ESB.19. | Oprogramowanie będzie zawierało opis proponowanego systemu kolejkowego, możliwości w zakresie ustanawiania QoS dla: usług, kolejek, komunikatów w kolejkach. |
| ESB.20. | Oprogramowanie zapewni realizację odpowiedniego poziomu bezpieczeństwa w zakresie:<br>a. uwierzytelniania<br>b. kontroli dostępu<br>c. zarządzania użytkownikami, grupami i rolami<br>d. tworzenia, przechowywania i walidacji certyfikatów, haseł, kluczy<br>e. audytowania zdarzeń bezpieczeństwa<br>f. wsparcia dla pojedynczego logowania SSO |
| ESB.21. | Oprogramowanie zapewni zgodność ze standardami WS-* a w szczególności z WS-Security, WS-Policy. |
| ESB.22. | Oprogramowanie zapewni dostępność mechanizmów uwierzytelniania i szyfrowania usług np. takich jak: użytkownik/hasło, passphrase, weryfikacja hostów, brak uwierzytelniania, tunelowanie wywołań SSL, certyfikaty X.509 |

| | |
|---|---|
| ESB.23. | Oprogramowanie zapewni możliwość ograniczenia czasu wywołań dla usług oraz użycia adapterów. |
| ESB.24. | Oprogramowanie będzie zawierało zestawienie adapterów do systemów i standardów zewnętrznych np.: NFS, pliki lokalne, HTTP, SMTP, FTP, JMS, MQ, JDBC, EDI, Oracle, DB2. |
| ESB.25. | Oprogramowanie zapewni obsługę komunikatów typu np.: SOAP, XML, FTP, SMTP. |
| ESB.26. | Oprogramowanie zapewni możliwość kontroli zmian wprowadzanych do ESB oraz ich cofnięcia. |
| ESB.27. | Oprogramowanie zapewni możliwość eksportu ustawień konfiguracyjnych i importu na innej instancji Szyny Usług. |
| ESB.28. | Oprogramowanie zapewni wsparcie dla replikacji sesji w pamięci pomiędzy wieloma instancjami węzłów Szyny Usług przy zapewnieniu wysokiej wydajności oraz możliwość replikacji sesji w trybie primary-secondary (czyli zarządzanie maksymalnie dwiema kopiami sesji użytkownika w klastrze). |
| ESB.29. | Oprogramowanie powinno mieć możliwość konfiguracji priorytetów obsługi żądań, priorytetów aplikacji i ich komponentów. Możliwość przypisywania reguł do użytkowników, aplikacji i ich komponentów (np. servlet'ów, EJB). Reguły powinny obejmować takie cechy jak: wagi (priorytety – np. % czasu procesorów gwarantowany dla aplikacji i/lub ich komponentów), czasy odpowiedzi, min/max liczba wątków, itp. |
| ESB.30. | Oprogramowanie powinno zawierać wbudowaną możliwość konfiguracji ochrony serwerów aplikacyjnych (i aplikacji) przed przeciążeniem. Dla przykładu: jeśli liczba żądań do serwera/aplikacji jest zbyt duża, serwer powinien przekierować nowe żądania do innych instancji w klastrze. |
| ESB.31. | Oprogramowanie powinno zapewnić możliwość zaprogramowania automatycznego restartu węzła i/lub komponentu w sytuacji zawieszenia (braku odpowiedzi), pojawienia się błędów o braku pamięci lub zbyt długiego wykonywania się wątków (stuck threads). |
| ESB.32. | Oprogramowanie powinno zapewnić możliwość rozdziału ruchu (protokołów) na różne interfejsy sieciowe (lub adresy IP). Np. możliwość rozdzielenia ruchu administracyjny/monitoringu od ruchu aplikacyjnego od ruchu związanego z funkcjonowaniem klastra (replikacja sesji) – powinna istnieć możliwość przesyłania danych związane z tymi funkcjami poprzez inne karty sieciowe/podsieci. |
| ESB.33. | Oprogramowanie powinno zawierać wbudowaną możliwość klastrowania połączeń JDBC. |
| ESB.34. | Oprogramowanie powinno zawierać wbudowaną możliwość klastrowania JMS (w tym automatyczne przełączanie klientów JMS w momencie failover serwerów JMS) |
| ESB.35. | Oprogramowanie powinno zapewnić możliwość automatycznego i ręcznego restartu (migracji) instancji serwerów aplikacyjnych na innych fizycznych maszynach w razie awarii, wraz z przeniesieniem istotnych dla przetwarzania danych (np. zawartość kolejek (np. JMS, MQSeries), logi transakcji rozproszonych JTA). Automatyczna rekonfiguracja serwerów aplikacyjnych po restarcie (zmiana adresu IP, itp.) |
| ESB.36. | Oprogramowanie powinno zawierać wbudowane wsparcie dla specyfikacji JSR-88 – Deployment Plan (plany wdrożeń). |
| ESB.37. | Oprogramowanie powinno zawierać wbudowaną obsługę pól połączeń do baz danych z uwierzytelnieniem połączeń. Tworzenie pul połączeń JDBC, w których jest możliwość zmapowania użytkowników serwera aplikacyjnego na użytkowników zdefiniowanych w bazie danych. Powinna być możliwość wykonania mapowania typu „user id per connection". |
| ESB.38. | Oprogramowanie powinno mieć wbudowaną obsługę zaawansowanych mechanizmów kolejkowych: grupowanie komunikatów przesyłanych do JMS z gwarancją zachowania kolejności ich przetworzenia (konsumpcji) wynikającą z kolejności ich utworzenia (produkcji). |
| ESB.39. | Oprogramowanie powinno mieć wbudowaną obsługę zaawansowanych mechanizmów kolejkowych: możliwość łączenia komunikatów w jednostki (grupy), a następnie przetwarzanie jednostek. Klient nie może przetwarzać danej jednostki, dopóki nie pojawią się wszystkie komunikaty wchodzące w skład danej jednostki. Przetwarzanie różnych jednostek (niezależnych od siebie grup komunikatów) powinno być jednak możliwe. |
| ESB.40. | Oprogramowanie powinno zapewnić wsparcie w zakresie wywołań i komunikacji z aplikacjami napisanych w języku innym niż JAVA np. C, .Net, C#. |
| ESB.41. | Oprogramowanie powinno zawierać wbudowany mechanizm automatycznej naprawy transakcji (transaction recovery) podczas restartu serwera aplikacyjnego. |

| | |
|---|---|
| ESB.42. | Oprogramowanie powinno zawierać opisaną w dokumentacji (wraz z przykładami) możliwość tworzenia własnych implementacji usług bezpieczeństwa: uwierzytelnienia, autoryzacji, mapowania ról, mapowania uwierzytelnień, baz danych kluczy/certyfikatów, walidacji poprawności kluczy/certyfikatów (CLV/CLR), audytowania. |
| ESB.43. | Oprogramowanie powinno zapewniać obsługę specyfikacji:<br>a. Java Authentication and Authorization Service (JAAS),<br>b. Java Secure Sockets Extensions (JSSE),<br>c. Java Cryptography Extensions (JCE),<br>d. Java Authorization Contract for Containers (JACC) |
| ESB.44. | Oprogramowanie powinno zawierać wbudowaną obsługę standardów SAML 1.1, SAML 2.0 lub wyższych. |
| ESB.45. | Oprogramowanie powinno zawierać wbudowane API do funkcjonalności przeszukiwania i walidacji certyfikatów X.509 (CLV – Certificate Lookup and Validation). |
| ESB.46. | Oprogramowanie powinno zapewnić obsługę mechanizmów autoryzacji i mapowania ról przy użyciu standardu XACML 2.0. |
| ESB.47. | Oprogramowanie powinno zapewnić możliwość konfiguracji dynamicznego członkowstwa ról, np. uwzględniającego datę i czas, zawartość wybranych elementów w komunikatach SOAP (Web services), wartość atrybutów żądań HTTP, wartość atrybutów sesji HTTP, czy parametrów metod EJB. |
| ESB.48. | Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-ReliableMessaging 1.1 i WS-ReliableMessaging Policy 1.1. |
| ESB.49. | Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-Trust 1.3. |
| ESB.50. | Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-SecureConversation 1.3. |
| ESB.51. | Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-Security 1.1. |
| ESB.52. | Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-SecurityPolicy 1.2. |
| ESB.53. | Oprogramowanie powinno zawierać wbudowaną obsługę asynchronicznych Web services. |
| ESB.54. | Oprogramowanie powinno zawierać wbudowaną obsługę Web services, które mogą wykonywać operacje na kliencie (callback Web service). |
| ESB.55. | Oprogramowanie powinno zawierać wbudowaną obsługę standardu Web Service MTOM\XOP – SOAP Message Transmission Optimization MechanAplikacja/XML- binary Optimized Packaging. |
| ESB.56. | Oprogramowanie powinno zawierać wbudowane wsparcie do udostępniania Web services typu REST. |
| ESB.57. | Oprogramowanie powinno zawierać wbudowane wsparcie dla buforowanego wywoływania Web services. |
| ESB.58. | Oprogramowanie powinno współpracować bez konieczności dokonywania integracji w trakcie wdrożenia z oferowaną infrastrukturą cache w zakresie przechowywania odpowiedzi (rezultatów) wynikających wywołania usług typu WebServices. |
| ESB.59. | Oprogramowanie dzięki integracji z oferowaną infrastrukturą cache powinno wspierać scenariusz, gdzie odpowiedz (rezultat) wynikająca z wywołania usługi typu WebService jest możliwa do uzyskania mimo awarii aplikacji, z której ta usługa korzysta |
| ESB.60. | Oprogramowanie powinno zawierać wbudowane wsparcie dla zewnętrznych dostawców usług kolejkowych wraz z przenoszeniem kontekstów security i transakcyjnego. |
| ESB.61. | Oprogramowanie powinno zawierać wbudowany moduł do diagnostyki pracy serwera aplikacyjnego i uruchomionych w nim aplikacji. Możliwość dynamicznego dodawania poprzez konfigurację własnego kodu diagnostycznego do określonych miejsc w aplikacji i jej komponentach. |

### 5.7.2 Silnik procesów biznesowych

Poniżej przedstawiono wymagania dla silnika procesów biznesowych

| ID wymagania | Opis wymagania |
|---|---|

| | |
|---|---|
| BPM.1. | Oprogramowanie do zarządzania procesami biznesowymi powinno odpowiadać za kontrolę sekwencyjności etapów procesów biznesowych oraz generowanie interfejsu dla użytkowników biorących udział w procesach. Powinno ono dostarczać całemu systemowi zbioru pojęć, zbioru struktur, relacji oraz dozwolonych operacji na nim oraz na jego elementach. Zadaniem oprogramowanie będzie przechowywanie definicji wszystkich obiektów systemu, ich parametrów, wzajemnych relacji pomiędzy nimi oraz zestaw metod wykonywanych na w/w obiektach. |
| BPM.2. | Oprogramowanie będzie posiadało silnik procesów biznesowych oparty o serwerze aplikacji zgodnym ze standardem JEE (Java Enterprise Edition). |
| BPM.3. | Oprogramowanie będzie posiadało interfejs użytkownika dostępny poprzez przeglądarkę internetową. |
| BPM.4. | Oprogramowanie powinno umożliwić uruchamianie procesów zawierających kroki manualne jak i zautomatyzowane. |
| BPM.5. | Powinno zawierać narzędzie do modelowania procesów, ich analizy, optymalizacji oraz uruchamiania procesów. Powinno także zawierać elementy odpowiedzialne za monitorowanie procesów. |
| BPM.6. | Oprogramowanie warstwy Zarządzania Procesami Biznesowymi powinno odpowiadać za orkiestrację procesów z uwzględnieniem użytkowników, struktury organizacyjnej, aplikacji i systemów zewnętrznych. Łączy się to z nadawaniem uprawnień użytkownikom sytemu. Uprawnienia powinny być przechowywane w zewnętrznym repozytorium zgodnym z LDAP. |
| BPM.7. | Oprogramowanie musi pozwalać na modelowanie struktur organizacyjnych. |
| BPM.8. | Oprogramowanie będzie posiadało interfejs graficzny, umożliwiający projektowanie procesów w postaci diagramów, uwzględniających aktorów biorących udział w procesie (role), opisujące typ realizowanej czynności, wykorzystywane aplikacje i dokumenty oraz zadania przez nich wykonywane. |
| BPM.9. | Oprogramowanie umożliwi wprowadzanie opisu procesów a w szczególności:<br>a. Początku i końca procesu.<br>b. Celu procesu, w tym poprzez opis tekstowy.<br>c. Nazwy procesu.<br>d. Aktywnych łączników do innych modeli procesów.<br>e. Określenie osoby zarządzającej procesem. |
| BPM.10. | Oprogramowanie umożliwi modelowanie w narzędziu hierarchii procesów i funkcji. |
| BPM.11. | Oprogramowanie umożliwi budowanie w narzędziu map procesów przez zespół kilku osób równolegle. |
| BPM.12. | Oprogramowanie umożliwi tworzenia w narzędziu map procesów typu "swimlane" (działania w pionowych lub poziomych torach dla jednostek/komórek organizacyjnych). |
| BPM.13. | Oprogramowanie umożliwi tworzenie w narzędziu hierarchicznych struktur danych. |
| BPM.14. | Oprogramowanie umożliwi eksportowanie w narzędziu procesów np. na portal procesowy (portal WWW). |
| BPM.15. | Oprogramowanie umożliwi przeprowadzenie w narzędziu symulacji zmian procesu pod kątem ilościowym np. skrócenie czasu obsługi procesu. |
| BPM.16. | Oprogramowanie umożliwi przeprowadzenie w narzędziu symulacji zmian procesu pod kątem jakościowym np. usunięcie realizowanych czynności w procesie. |
| BPM.17. | Oprogramowanie umożliwi wykorzystanie w narzędziu symulacji biorąc pod uwagę kalendarz pracy dla czynności systemowych. |
| BPM.18. | Oprogramowanie umożliwi wykonanie w narzędziu symulacji w odniesieniu do utworzonych modeli procesów. |
| BPM.19. | Oprogramowanie umożliwi przeprowadzenie w narzędziu symulacji polegających na:<br>a. Weryfikacji czasochłonności procesu i jego poszczególnych etapów.<br>b. Wykonaniu analiz kosztowych procesu.<br>c. Wykonaniu analiz dotyczących zasobów (ludzkich/systemowych) w procesie. |
| BPM.20. | Oprogramowanie umożliwi monitorowanie danych w narzędziu w czasie rzeczywistym, w tym dotyczących:<br>a. Danych, które powinny być prezentowane w formie graficznej (wykresy) oraz/lub w formie tabelarycznej (listy). |

| | |
|---|---|
| | b. Umożliwi tworzenie zestawień hierarchicznych (tzw. drill down) – pozwalających na przejście od informacji ogólnej na poziom bardziej szczegółowy. |
| BPM.21. | Oprogramowanie umożliwi prezentację w narzędziu danych poprzez ich wizualizację na wielu poziomach szczegółowości, w postaci interaktywnych list zestawień, wykresów, zestawień wskaźnikowych (kokpitów menadżerskich). |
| BPM.22. | Oprogramowanie umożliw prezentację w narzędziu wybranych KPI z wartością faktyczną i wartością oczekiwaną . |
| BPM.23. | Oprogramowanie umożliwi generowanie w narzędziu alertów w postaci komunikatów, wiadomości mailowych oraz automatycznego uruchamiania procesów reagując na raportowane zdarzenia. |
| BPM.24. | Oprogramowanie umożliwi publikowanie w narzędziu/rozwiązaniu modeli procesowych w postaci stron WWW - „Portal procesowy”. |
| BPM.25. | Oprogramowanie umożliwi prezentację w narzędziu/rozwiązaniu w formie graficznej (mapa np. w formacie: jpg) całego procesu. W przypadku procesów głównych i podprocesów, umożliwi prezentację wg podziału procesów i ich logicznego powiązania. |
| BPM.26. | Oprogramowanie umożliwi importowanie do narzędzia/rozwiązania gotowych procesów z narzędzi do modelowania. |
| BPM.27. | Oprogramowanie umożliwi przekształcenia map procesów w postać możliwą do dalszej dystrybucji np. do postaci tabelarycznej procedury i eksportu jej do formatu MS Word lub PDF. |
| BPM.28. | Oprogramowanie umożliwi zastosowanie notacji BPMN. |
| BPM.29. | Oprogramowanie umożliwi przekształcenia, zapis, eksport oraz import modeli biznesowych (BPMN) w formatach np.: XPDL, BPEL. |
| BPM.30. | Oprogramowanie umożliwi tworzenie procesu w oparciu o gotowe komponenty logiki jak i usługi – współpraca z UDDI. |
| BPM.31. | Oprogramowanie umożliwi orkiestrację procesów z uwzględnieniem zadań wykonywanych przez użytkowników (lub grup użytkowników) oraz z wykorzystaniem funkcjonalności istniejących aplikacji i systemów. |
| BPM.32. | Oprogramowanie umożliwi synchroniczne lub asynchroniczne wywoływanie procesów na podstawie zdarzeń zewnętrznych. |
| BPM.33. | Oprogramowanie umożliwi uruchamianie procesu w wyniku zdarzenia w postaci pojawienia się w odpowiednim katalogu pliku lub przesyłki email. |
| BPM.34. | Oprogramowanie umożliwi obsługę procesów wymagających interakcji z użytkownikiem. |
| BPM.35. | Oprogramowanie będzie posiadało mechanizm notyfikacji użytkowników pozwalający powiadamiać odpowiednie osoby o zdarzeniach zachodzących w procesie. |
| BPM.36. | Oprogramowanie będzie posiadało generator interfejsu użytkownika – pozwoli na automatyczną generację formularzy na podstawie struktur danych przechowujących informacje w procesie. |
| BPM.37. | Oprogramowanie będzie posiadało mechanizmy walidacji danych wprowadzanych przez użytkownika. |
| BPM.38. | Oprogramowanie będzie posiadało mechanizmy kontroli terminów wykonania poszczególnych zadań/etapów w procesie (deadlines). |
| BPM.39. | Oprogramowanie będzie posiadało mechanizmy automatycznego przekierowania zadań w procesie pod nieobecność użytkownika (urlop, choroba). |
| BPM.40. | Oprogramowanie umożliwi zmiany sposobu działania procesu "w locie" (bez ingerencji programistycznej) przez uprawnionych użytkowników (np. odebranie zadania, cofnięcie procesu do określonego punktu). |
| BPM.41. | Oprogramowanie będzie posiadało interfejs użytkownika umożliwiający personalizację stron przez użytkowników. |
| BPM.42. | Oprogramowanie umożliwi wielokrotne użycie elementów interfejsu w innych aplikacjach - wsparcie dla JSR-168 (portlety) |
| BPM.43. | Oprogramowanie umożliwi obieg dokumentów oraz generowanie formularzy na bazie danych procesu. |
| BPM.44. | Oprogramowanie będzie zawierało silnik procesowy pozwalający na wykonywanie w środowisku produkcyjnym zaprojektowanych modeli procesów. Silnik procesowy powinien wspierać standardy opisu procesów: BPEL, XPDL. |

| | |
|---|---|
| BPM.45. | Oprogramowanie powinno uwzględniać wykorzystanie reguł biznesowych jako mechanizmu do definiowania polityk biznesowych. |
| BPM.46. | Oprogramowanie powinno zawierać interfejs dostępowy silnika reguł biznesowych zgodny z JSR-94. |
| BPM.47. | Oprogramowanie umożliwi równoległe procesowania różnych wersji tego samego procesu (w przypadku, gdy wdrożono nową wersję, ale istnieją instancje rozpoczęte jeszcze na starej wersji). |
| BPM.48. | Oprogramowanie umożliwi wystawianie interfejsów do utworzonych procesów biznesowych (np. w postaci web service'u pozwalającego uruchomić proces) i wystawienie go na Szynie Usługowej. |
| BPM.49. | Oprogramowanie umożliwi budowanie projektów integracyjnych w oparciu o standard SCA (Service Component Architecture). |
| BPM.50. | Oprogramowanie umożliwi zdefiniowanie w ramach jednego kompozytu SCA zestawu procesów integracyjnych wraz hierarchią wywołań pomiędzy nimi (procesy nadrzędne i pod-procesy). |
| BPM.51. | Oprogramowanie umożliwi w ramach kompozytów SCA walidację, filtrowanie i transformację komunikatów przychodzących, a następnie przekierowanie ich do odpowiedniego procesu integracyjnego. |
| BPM.52. | Oprogramowanie umożliwi orkiestrację usług w postaci procesów integracyjnych zgodnych ze standardem WS-BPEL 2.0 |
| BPM.53. | Oprogramowanie w momencie przekazania musi mieć możliwość uruchomienia następujących usług atomowych:<br>a. Wystawienie faktury za świadczenie komercyjne<br>b. Rejestracja klienta/pacjenta<br>c. Kartoteka klienta/pacjenta<br>d. Przypisanie elementów majątku trwałego do struktury organizacyjnej<br>e. Budowanie struktury organizacyjnej |
| ESB.62. | Oprogramowanie musi być dostarczone z licencjami umożliwiającymi jego uruchomienie na infrastrukturze określonej w zestawieniu ilościowym, przy czym zakłada się, że liczba licencji nie będzie wystarczająca do obsadzenia całości serwera, dlatego dopuszcza się zastosowanie wirtualizacji umożliwiającej pracę oprogramowania w liczbie zakładanej z zestawieniu ilościowym. |

# 6 Wymagania ogólne

Dla wymagań ogólnych przyjęte zostały następujące wytyczne do budowania identyfikatorów:

- DOK – wymagania dla dokumentacji
- WDR – wdrożenie dostarczonego rozwiązania
- ESK – wytyczne dla eksploatacji
- WSP – II i III linii wsparcia
- INS – wymagania dla instruktaży stanowiskowych

## 6.1 Dokumentacja

| ID wymagania | Opis wymagania |
|---|---|
| DOK.1 | Wykonawca zobowiązany jest do przekazania w wersji papierowej 1 egzemplarz oraz wersji elektronicznej po 2 egzemplarze dokumentacji wymaganej poniższymi wymaganiami na trwałym nośniku (np. CD lub DVD lub pendrive, itp.).<br>Na każdym nośniku dodatkowo poza przekazywaną dokumentacją musi być dostępny plik zawierający poniższy wykaz:<br>• Nazwa pliku (tożsama nazwie dokumentu)<br>• Wersja pliku (tożsama wersji dokumentu)<br>• Data opracowania pliku<br>• Autorzy dokumentu |
| DOK.2 | Wykonawca przeprowadzi Analizę przedwdrożeniową. |
| DOK.3 | Wykonawca w ramach Analizy przedwdrożeniowej opracuje Harmonogram wdrożenia, który zawierać będzie co najmniej:<br>• Plan dostaw infrastruktury sprzętowej oraz sieciowej (w postaci diagramu Gantta ze wskazaniem planowanych dat oraz czasu trwania dostaw)<br>• Plan kolejności instalacji i wdrożenia poszczególnych komponentów (aaplikacji infrastrukturalnych, oprogramowania standardowego, itd.) |
| DOK.4 | Wykonawca opracuje Dokumentację projektową na którą składają się co najmniej:<br>• Zaktualizowany Projekt techniczny<br>• Dokumentację techniczną powykonawczą<br>• Dokumentacja użytkownika<br>• Dokumentację administratora<br>• Dokumentację testową |
| DOK.5 | Wykonawca w ramach Analizy przedwdrożeniowej musi opracować szczegółowy Projekt techniczny dostarczanego rozwiązania umożliwiający instalację i konfigurację wszystkich wymaganych komponentów oraz aplikacji. Jako Projekt techniczny rozumie się dokumentację opisującą szczegółową konfigurację komponentów, ich wzajemnych relacji i powiązań umożliwiających zainstalowanie, uruchomienie i poprawną pracę poszczególnych aplikacji i systemów.<br>Projekt techniczny musi obejmować co najmniej następujące informacje:<br>• Model architektury logicznej (listę i opis komponentów, wraz z wykazem oprogramowania, za pomocą którego dany komponent jest realizowany, interfejsy logiczne pomiędzy komponentami Systemu)<br>• Model architektury technicznej (wykaz oprogramowania standardowego, wykaz oprogramowania dedykowanego budowanego w ramach niniejszego postępowania, konfigurację oprogramowania, opis interfejsów z systemami zewnętrznymi wraz ze specyfikacją komunikacji, rozmieszczenie oprogramowania w architekturze fizycznej)<br>• Architektura fizyczna (opis dostarczonego sprzętu w tym nazwa/typ urządzenia, rola w systemie, parametry, numer seryjny; architektura fizyczna rozwiązania, architektura sieciowa, projekt instalacji dostarczanego rozwiązania, konfigurację urządzeń) |
| DOK.6 | Wykonawca musi opracować Dokumentację administratora, która zawierać będzie co najmniej: |

| | |
|---|---|
| | • Procedury administracyjne<br>• Procedury instalacji i konfiguracji<br>• Procedury bieżących działań administracyjnych<br>• Procedury okresowych/planowanych działań administracyjnych<br>• Procedury aktualizacji standardowych elementów dostarczonego rozwiązania<br>• Procedury awaryjne (w tym wykonanie kopii bezpieczeństwa – pełnej oraz przyrostowej, postępowanie w przypadku awarii systemu)<br>• Procedur Distater Recovery ze scenariuszami awarii oraz procedur działań odtworzeniowych i uruchomieniowych mających na celu zminimalizowanie strat danych oraz zminimalizowanie czasu niedostępności usług |
| DOK.7 | Wykonawca musi opracować dokumentację testów, na którą składają się co najmniej:<br>• scenariusze testowe umożliwiające weryfikację poprawności instalacji i konfiguracji zainstalowanych komponentów. Za kompletność scenariuszy testowych odpowiada Wykonawca.<br>• Plan testów<br>• Raport z testów (zgodny z zaakceptowaną Procedurą testów) |
| DOK.8 | Plan testów musi zawierać co najmniej:<br>• proponowany czas trwania testu<br>• podstawowe informacje na temat przedmiotu testów,<br>• zakres testów |
| DOK.9 | Wykonawca musi opracować szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis konfiguracji zainstalowanych komponentów poszczególnych aplikacji oraz systemów. |
| DOK.10 | Wykonawca dostarczy równocześnie Zamawiającemu pełną dokumentację standardowo dostarczaną przez producentów do dostarczonego sprzętu oraz oprogramowania. |

## 6.2 Wdrożenie

Poniżej przedstawiono wymagania dla Wdrożenia.

| ID wymagania | Opis wymagania |
|---|---|
| WDR.1 | Wszelkie koszty związane z dostawą sprzętu do wskazanego przez Zamawiającego miejsca, a także instalacją sprzętu oraz oprogramowania ponosi Wykonawca. |
| WDR.2 | Wykonawca dostarczy sprzęt wraz z niezbędnym okablowaniem, dokumentacją techniczno-eksploatacyjną, certyfikatami bezpieczeństwa oraz dokumentami potwierdzającymi udzielenie Zamawiającemu gwarancji na te urządzenia. |
| WDR.3 | Instalacja sprzętu oraz oprogramowania, a także jego konfiguracja musi spełniać wymagania zawarte w Umowie. |
| WDR.4 | Wykonawca musi zainstalować i skonfigurować wszystkie komponenty zgodnie z zaakceptowanym szczegółowym projektem technicznym. |
| WDR.5 | Wykonawca będzie dostarczał wymagane elementy rozwiązania (w tym sprzęt serwerowy, sprzęt sieciowy, itd.) sukcesywnie w ilości niezbędnej do prowadzenia prac instalacyjnych zgodnie z harmonogramem. |
| WDR.6 | Wykonawca ma zapewnić wniesienie dostarczonego sprzętu do miejsca wskazanego przez Zamawiającego. |
| WDR.7 | Wykonawca będzie dostarczał sprzęt sieciowy oraz serwerowy sukcesywnie w terminie bezpośrednio poprzedzającym jego instalację i w sposób dopasowany do możliwości logistycznych Zamawiającego. Zakres i wielkości dostaw należy każdorazowo uzgodnić z Zamawiającym. |
| WDR.8 | Za przechowywanie narzędzi i materiałów (w tym pasywnego i aktywnego sprzętu sieciowego) w miejscu instalacji odpowiada Wykonawca. Wykonawca zobowiązany jest zagwarantować przechowywanie materiałów zgodnie z wymaganiami producenta. |
| WDR.9 | Wykonawca zobowiązany jest do instalacji wymaganego oprogramowania systemowego i narzędziowego na dostarczonym i skonfigurowanym uprzednio sprzęcie. Po zakończeniu |

| | |
|---|---|
| | instalacji, zainstalowane oprogramowanie musi zostać skonfigurowane tak aby działało poprawnie zgodnie z jego przeznaczeniem. |
| WDR.10 | Wykonawca musi przeprowadzić testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów.<br>Zakres testów obejmuje:<br>• Testy funkcjonalne<br>• Testy integracyjne<br>• Testy bezpieczeństwa |
| WDR.11 | Wykonawca musi opracować szczegółowe procedury eksploatacyjne wdrożonych komponentów i systemów/aplikacji.<br>Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji systemu operacyjnego. Procedury muszą obejmować wszystkie czynności konieczne do realizowania w celu monitorowania i utrzymania dostarczonych komponentów poszczególnych systemów oraz aplikacji w poprawnym działaniu i zgodności z najnowszymi wersjami. |
| WDR.12 | Po zakończeniu wdrożenia sprzętu Wykonawca musi przedstawić „Raport z dostaw sprzętu", który zawierać powinien co najmniej:<br>a. opis wszystkich elementów sprzętowych oraz dla każdego z nich wyspecyfikowane co najmniej:<br>• nazwę,<br>• nazwę własną danego elementu sprzętowego (wraz z jego modelem),<br>• nr seryjny elementu sprzętowego (ewentualne inne istotne identyfikatory określone przez Wykonawcę lub producenta),<br>• lokalizację zainstalowanego sprzętu np. w serwerowni (rysunek poglądowy lub opis),<br>• datę produkcji elementu sprzętowego,<br>• koszt elementu sprzętowego wyrażony w polskich złotych netto oraz brutto.<br>b. deklarację, że dostarczony sprzęt jest nowy, wolny od wad, pochodzi z legalnego źródła i jest dopuszczony w Polsce do obrotu, oraz spełnia wszystkie wymogi określone przez Zamawiającego w SIWZ. |

Wykonawca musi wykonać następujące zadania wdrożeniowe:

| ID wymagania | Opis wymagania |
|---|---|
| WDR.13 | Instalacja i konfiguracja aplikacji infrastrukturalnych oraz oprogramowania standardowego na środowisku uzgodnionym z Zamawiającym |
| WDR.14 | Instalacja i konfiguracja systemów operacyjnych wyspecyfikowanych przez Zamawiającego, na środowisku przez niego wskazanym oraz zgodnie z wytycznymi Zamawiającego |
| WDR.15 | Instalacja i konfiguracja systemów baz danych wyspecyfikowanych przez Zamawiającego, na środowisku przez niego wskazanym oraz zgodnie z wytycznymi Zamawiającego |
| WDR.16 | Instalacja oraz konfiguracja dostarczonych systemów identyfikacji użytkowników wyspecyfikowanych przez Zamawiającego, na środowisku przez niego wskazanym oraz zgodnie z wytycznymi Zamawiającego |
| WDR.17 | Instalacja i konfiguracja serwerów aplikacyjnych wyspecyfikowanych przez Zamawiającego, na środowisku przez niego wskazanym oraz zgodnie z wytycznymi Zamawiającego |
| WDR.18 | Instalacja i konfiguracja oprogramowania narzędziowego do zarządzania dostarczoną infrastrukturą sprzętową wyspecyfikowanego przez Zamawiającego, na środowisku przez niego wskazanym oraz zgodnie z wytycznymi Zamawiającego |

## 6.3 Wytyczne dla eksploatacji

Poniżej przedstawiono wymagania dla eksploatacji dostarczonego rozwiązania w trakcie obowiązywania okresu gwarancji.

| ID wymagania | Opis wymagania |
|---|---|
| ESK.1 | Wykonawca musi informować Zamawiającego pisemnie o wszystkich wymaganych aktualizacjach wszystkich systemów i komponentów dostarczonych w niniejszym zamówieniu. |
| ESK.2 | Wykonawca zobowiązany jest zapewnić dostęp Zamawiającemu do aktualizacji oprogramowania standardowego oraz dostarczyć opis procedur pozyskiwania informacji o dostępności aktualizacji oraz sposobu instalacji aktualizacji. |
| ESK.3 | Wykonawca musi zapewnić zdalny dostęp do środowiska. Zdalny dostęp musi być realizowany z wykorzystaniem bezpiecznego kanału transmisji opartego o VPN. |
| ESK.4 | Wykonawca zapewni konsultacje na potrzeby Zamawiającego w ramach eksploatacji zgodnie z wytycznymi Umowy. |

## 6.4 Wsparcie

Wsparcie musi być zorganizowane zgodnie z modelem ITIL w wersji 3 i musi być podzielone na 3 linie wsparcia. Pierwsza linia wsparcia (kontakt z klientem) będzie realizowany przez Zamawiającego. Wykonawca musi świadczyć usługi wsparcia dla II oraz III linii wsparcia.

Poniżej przedstawiono wymagania dla II i III linii wsparcia, która musi być świadczona przez Wykonawcę w okresie trwania gwarancji dla poszczególnych systemów oraz aplikacji.

| ID wymagania | Opis wymagania |
|---|---|
| WSP.1 | Wykonawca zobowiązany jest zapewnić wsparcie techniczne dla dostarczanych komponentów. Wsparcie musi być dostępne w języku polskim poprzez konsultacje na miejscu (w lokalizacji wskazanej przez Zamawiającego na terenie Wrocławia), e-mail oraz połączenia telefoniczne wg taryfy lokalnej.<br>W ramach wsparcia technicznego Wykonawca będzie zobowiązany do:<br>• świadczenia merytorycznego wsparcia podczas instalacji nowych wersji oprogramowania,<br>• uczestniczenia w procesie lokalizowania błędów w działaniu poszczególnych aplikacji i systemów,<br>• usuwania wszystkich błędów. |
| WSP.2 | Wykonawca zapewni II oraz III linię wsparcia. Zamawiający w swoich strukturach, lub zleci to zewnętrznemu podmiotowi, będzie prowadzić I linię wsparcia.<br>Zgłoszenia, które dotyczyć będą błędów bądź problemów z systemami/aplikacjami bądź sprzętem dostarczonym w niniejszym zamówieniu będą kierowane do Wykonawcy poprzez kanał zgłoszeń (narzędzie pozwalające na zgłaszanie oraz obsługę zgłoszeń).<br>Za przypisanie kategorii błędu odpowiada Zamawiający (w ramach I linii wsparcia). |
| WSP.3 | Wsparcie techniczne musi zawierać co najmniej:<br>• wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz dystrybutora sprzętu,<br>• wymianę uszkodzonego sprzętu (producent wysyła sprzęt nie później niż następnego dnia roboczego),<br>• dostęp do nowych wersji oprogramowania, w tym aktualizację baz, definicji lub konfiguracji (np. bazy sygnatur ataków dla oprogramowania antywirusowego),<br>• dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. |
| WSP.4 | Wykonawca dostarczy narzędzie pozwalające na zgłaszanie oraz obsługę zgłoszeń (zapytań, błędów, itd.) od użytkowników. Narzędzie do obsługi błędów musi zapewniać równoczesną pracę co najmniej 50 użytkowników końcowych.<br>Wdrożone narzędzie musi mieć możliwość zwiększenia liczby użytkowników równocześnie korzystających z narzędzia (np. poprzez dokupienie dodatkowych licencji).<br>Narzędzie musi pozwalać co najmniej na:<br>• Wprowadzenie zgłoszenia (błędu, pytania, itd.). |

| | |
|---|---|
| | • Przypisanie zgłoszenia (automatyczne bądź ręczne) do wybranej roli.<br>• Pełną obsługę zgłoszenia (przekazywanie pomiędzy użytkownikami, zamknięcie oraz ponowne otworzenie zgłoszenia, dodawanie komentarzy do zgłoszenia, obserwowanie zgłoszenia, itd.).<br>• Definiowanie workflow (procesu obsługi zgłoszenia wg ustalonych parametrów np. typ zgłoszenia – błąd, wniosek o zmianę, wniosek o modyfikację uprawnień; priorytet zgłoszenia, itd.).<br>• Zarządzanie użytkownikami oraz uprawnieniami.<br>Narzędzie musi być dostępne poprzez interfejs www.<br>Wykonawca odpowiada za opracowanie materiałów dla użytkowników tj. instrukcji użytkowania narzędzia do obsługi błędów zawierającej zrzuty z ekranów wraz z opisem czynności jakie użytkownik musi podjąć dla danej funkcji. |
| WSP.5 | Wykonawca zapewni konsultacje dla zespołu Zamawiającego w ramach Asysty stanowiskowej. Konsultacje będą zlecane przez Zamawiającego oficjalnym kanałem komunikacji (pismem bądź faksem). Zlecenie będzie obejmować:<br>• zakres konsultacji<br>• szacowany czas konsultacji |

## 6.5 Instruktaże stanowiskowe

Poniżej przedstawiono wymagania dla Instruktaży stanowiskowych.

| ID wymagania | Opis wymagania |
|---|---|
| INST.1 | Wykonawca musi zapewnić szkolenia/instruktaże stanowiskowe z dostarczonych:<br>• Aplikacji infrastrukturalnych<br>• Infrastruktury technicznej |
| INST.2 | Szkolenia/instruktaże stanowiskowe muszą zostać przeprowadzone dla:<br>• Co najmniej 2 administratorów dla każdej aplikacji infrastrukturalnej<br>• Co najmniej 2 administratorów dla infrastruktury technicznej w podziale na sekcje wskazane w rozdziale 5. |
| INST.3 | Wykonawca zobowiązany jest przygotować materiały szkoleniowe, które podlegać będą akceptacji Zamawiającego. Materiały szkoleniowe muszą być dostępne w wersji MS Office lub MS Power Point lub PDF oraz jako materiały e-learning i muszą zostać udostępnione w ramach Bazy Wiedzy. Materiały szkoleniowe muszą zostać przedstawione do akceptacji Zamawiającemu na 5 dni przed rozpoczęciem szkoleń. |
| INST.4 | Wykonawca musi na co najmniej 2 tygodnie przed terminem rozpoczęcia szkoleń przedstawić Zamawiającemu do akceptacji szczegółowy program szkoleń.<br>Program szkolenia musi pozwalać na kompleksowe zapoznanie uczestników z funkcjonalnościami aplikacji.<br>Wszystkie szkolenia zakończone zostaną ankietą oceniającą przebieg szkolenia. Skala oceniająca szkolenia to 1—5, wymagane jest aby średnia ocen była równa lub przekraczała 3,5. W przypadku gdy ocena szkolenia będzie poniżej 3,5 Wykonawca zobowiązany jest do ponownego przeprowadzenia całego szkolenia. |
| INST.5 | Wykonawca po wykonaniu instruktażu zobowiązany jest przedstawić Zamawiającemu (w ciągu 2 dni roboczych) listę obecności uczestników podpisaną przez każdego z nich oraz wypełnione przez uczestników ankiety oceny instruktażu. |
| INST.6 | Zamawiający ma prawo do oddelegowania wizytatora, który dokona oceny sposobu przeprowadzenia instruktażu. Podczas instruktażu wizytator nie będzie traktowany jak uczestnik. |
| INST.7 | Czas trwania szkoleń z zakresu aplikacji infrastrukturalnych dla administratorów:<br>• Co najmniej 6 godzin zegarowych liczonych bez przerw dla każdej aplikacji |
| INST.8 | Czas trwania szkoleń z zakresu infrastruktury technicznej: |

| | |
|---|---|
| | Co najmniej 6 godzin zegarowych liczonych bez przerw dla infrastruktury wskazanej w sekcjach rozdziału 5 |
| INST.9 | Szkolenia odbędą się w lokalizacji wskazanej przez Zamawiającego na terenie Wrocławia – Zamawiający zapewnia salę szkoleniową. |
| INST.10 | Wykonawca odpowiada za catering w trakcie szkolenia (kawa, herbata, woda oraz ciastka). |
| INST.11 | Wykonawca odpowiada za zapewnienie niezbędnego sprzętu (np. laptopów i rzutnika) oraz materiałów szkoleniowych dla uczestników szkoleń. |
| INST.12 | Wykonawca odpowiada za przygotowanie środowiska szkoleniowego, które pozwoli na przeprowadzenie instruktaży stanowiskowych. |
| INST.13 | W instruktażach mogą uczestniczyć pracownicy Zamawiającego lub osoby z podmiotów przez niego wskazanych. |