Zmodyfikowany Załącznik nr 3.1 do SWZ

Dotyczy Pakietu nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

Część 2 - Zakup usługi i wdrożenie środowiska odtworzeniowego działającego w modelu chmurowym

Zakup usługi i wdrożenie środowiska działającego w modelu chmurowym, posłuży wykonywaniu kopii zapasowych oraz odtwarzaniu (na potrzeby testów lub bieżącej pracy) systemów dziedzinowych takich jak HIS, ERP, LIS. W zakresie usługi możliwe będzie dodatkowo wykorzystanie środowiska chmurowego do roli środowiska produkcyjnego (w przypadku niedostępności podstawowego środowiska lokalnego szpitala).

System ma zapewnić

a) kopie baz danych takich jak HIS, ERP, LIS,

b) kopie maszyn wirtualnych,

c) kopie aplikacji i konfiguracji,

d) cykliczna weryfikacja możliwości odtworzenia środowiska,

e) testowanie wykonanych kopii (cyklicznego testowania odtwarzania systemów z kopii),

f) integrację systemu (usługi) z działającym u Zamawiającego systemem kopii bezpieczeństwa,

g) aktywny backup EDM z mechanizmami bezpiecznego udostępniania EDM poprzez Platformę P1 (funkcjonalność opcjonalna),

System przyczyni się do wsparcia rozwoju elektronicznej dokumentacji medycznej i e-usług dzięki zwiększeniu bezpieczeństwa informatycznego szpitala.

Ponadto Zadanie niniejsze obejmuje zakup dwóch licencji bazodanowych Oracle Standard Edition 2 - w wydaniu kompatybilnym z posiadanym przez Zamawiającego oprogramowaniem (w szczególności klasy HIS) oraz wymaganiami oferowanego rozwiązania chmurowego a także ich wdrożenie w miejsce posiadanych przez Zamawiającego niższych wersji (wydania). Zamawiający posiada licencje Oracle Database Standard Edition 2 (processsor perpetual – 2 szt.).

Realizacja zadania stanowi element przedsięwzięcia, polegającego na działaniach zwiększających poziom cyberbezpieczeństwa szpitala i bezpośrednio pozwoli spełnić wymogi wskaźnika D21G.R2.

Zapisy niniejszego dokumentu odnoszą się do rozwiązania chmurowego Oracle Cloud Infrastructure wskazanego jako rozwiązanie przykładowe z uwagi posiadania przez zamawiającego systemów firmy Asseco pracujących wyłącznie na środowisku bazodanowym Oracle. Zamawiający dopuszcza rozwiązania chmurowe (usługi) równoważne.

Za usługę równoważną do przedmiotu zamówienia Zamawiający uzna taką, która spełniać będzie poniższe warunki:

a) umożliwia dostęp do usług chmurowych typu Platform as a Services (PaaS) oraz Infrastructure as a Service (IaaS) bez określania, jakie to mają być usługi i bez konieczności oddzielnego zakupu

licencji (niezbędne do uruchomienia i funkcjonowania usługi licencje będą dostępne w modelu „License Included")

b) Zamawiający będzie mógł dowolnie zmieniać usługi, z jakich będzie korzystał w okresie realizacji zamówienia,

c) zakres zastosowania technologii zapewni Zamawiającemu możliwość implementacji funkcjonalności, które Zamawiający realizuje w oparciu o technologię Oracle, w szczególności umożliwi Zamawiającemu utrzymywanie systemu klasy HIS opartego o bazę danych Oracle, bez konieczności zakupu dodatkowych licencji, wykonywania dodatkowych prac dostosowawczych czy migracji,

d) nie będzie powodować zakłóceń pracy oprogramowania z zakresu technologii bazodanowej Oracle, z którym będzie współdziałało,

e) zapewni pełną, równoległą pracę w czasie rzeczywistym oraz pełną funkcjonalną zamienność technologii równoważnej z technologią Oracle,

f) umożliwi wskazanie miejsca przetwarzania danych na terenie Europejskiego Obszaru Gospodarczej (EOG, ang. European Economic Area) i uniemożliwi ich przekazanie przez procesora w jakiejkolwiek formie (np. backup, logi) poza ten obszar.

Zakres funkcjonalny:

Zamawiający oczekuje dostarczenia kompleksowego rozwiązania informatycznego, przeznaczonego do utrzymywania w chmurze w pełni funkcjonalnych replik posiadanych systemów HIS, LIS oraz ERP firmy Asseco, które zapewni następujące możliwości:

1. Utrzymywanie w chmurze bliźniaczego środowiska informatycznego, stanowiącego wierne i aktualne odwzorowanie środowiska lokalnego w zakresie danych bazodanowych oraz wszystkich komponentów funkcjonalnych w/w aplikacji Asseco (bliźniacze środowisko produkcyjne).
2. Automatyczne tworzenie przyrostowych kopii bezpieczeństwa baz danych w chmurowej usłudze (platformie) w celu realizacji backupu wykonywanego przez Zamawiającego z wykorzystaniem narzędzia RMAN. Baza danych przed przesłaniem do środowiska OCI będzie zaszyfrowana po stronie Zamawiającego. Wymagana jest możliwość przechowywania zaszyfrowanych backupów w OCI oraz ich odtwarzania na potrzeby weryfikacji poprawności backupu. Środowisko musi umożliwiać odtworzenie backupu bez konieczności pozyskiwania dodatkowych licencji bazodanowych. W ramach zamówienia Wykonawca zapewni konfigurację i uruchomienie backupu w środowisku chmurowym, konfigurację testów odtworzeniowych i raportowania, doradztwo techniczne przy konfiguracji środowiska oraz dokumentację wdrożeniową a Usługa udostępnienia środowiska chmurowego świadczona będzie zgodnie z warunkami i zasadami zawartymi w dokumencie „Oracle PaaS and IaaS Universal Credits Service Descriptions", publikowanymi przez dostawcę usługi chmurowej na stronie: http://www.oracle.com/us/corporate/contracts/paas-iaas-universal-credits-3940775.pdf, lub w oparciu o równoważny dokument. Wykonawca zobowiązany jest dostarczyć Zamawiającemu potwierdzenie nabycia praw do korzystania z usługi - potwierdzenie zostanie przekazane Zamawiającemu najpóźniej na moment podpisania protokołu odbioru (lub odpowiedniego etapu odbiorowego), potwierdzającego uruchomienie i gotowość usługi do eksploatacji..
3. Automatyczne i selektywne tworzenie przyrostowych kopii bezpieczeństwa wszystkich plików uruchomieniowych, plików konfiguracyjnych, bibliotek oraz pozostałych komponentów funkcjonalnych, składających się na aplikacje HIS, LIS oraz ERP.
4. Zamawiający nie dopuszcza rozwiązania opartego wyłącznie o kopie bezpieczeństwa obrazów maszyn wirtualnych serwerów, obrazów dysków czy też całych folderów – wymagane jest

rozwiązanie operujące na pojedynczych plikach lub komponentach funkcjonalnych w/w aplikacji, dające możliwość selektywnego tworzenia kopii bezpieczeństwa pojedynczych składników, np. aplikacji, modułów, wersji, konfiguracji, itp.

5. Dostarczone rozwiązanie musi umożliwiać automatyczne oraz na żądanie odkładanie w chmurze (tj. zewnętrznym data center) wszystkich w/w komponentów oraz danych bazodanowych.
6. W chmurze powinny być wydzielone miejsca na bezpieczne przechowywanie backupowanych zasobów oraz w pełni działającą replikę środowiska aplikacyjnego dla wszystkich w/w systemów Asseco. Praca w systemie chmurowym powinna być możliwa niezależnie od środowiska produkcyjnego Zamawiającego.
7. Środowisko chmurowe dla systemów Asseco musi posiadać identyczną konfigurację jak lokalne środowisko produkcyjne, tj. muszą w nim zostać zainstalowane, skonfigurowane oraz uruchomione wszystkie lokalnie działające elementy systemów Asseco.
8. Dostarczone rozwiązanie powinno zapewniać automatyczne aktualizowanie środowiska chmurowego równolegle z przeprowadzanymi aktualizacjami środowiska lokalnego systemów Asseco, tak by oba rozwiązania były zawsze identyczne w sensie konfiguracji oraz wersji działających modułów. Synchronizacja obu środowisk powinna się odbywać automatycznie, bez dodatkowej ingerencji administratora.
9. Wykonawca zobowiązany jest dostarczyć stosowne licencje dla baz danych uruchamianych w chmurze, zapewniających stałą synchronizację oraz uruchamianie w/w aplikacji Asseco, które z tych baz korzystają.
10. Wykonawca zobowiązany jest dostarczyć stosowne licencje wszystkich dodatkowych narzędzi, z których składa się jego rozwiązanie, np. systemy operacyjne Windows, licencje dostępowe CAL, licencje RDP, itp.
11. Środowisko chmurowe powinno zapewniać przechowywanie minimum trzech pełnych wersji środowiska lokalnego – zarówno danych bazodanowych, jak i w/w komponentów aplikacyjnych HIS, LIS oraz ERP. Dodatkowo, najbardziej aktualna z tych wersji powinna być zawsze gotowa do użycia (na wypadek konieczności produkcyjnego skorzystania z systemu chmurowego).
12. Wszystkie dane powinny być synchronizowane automatycznie, zgodnie z ustalonym harmonogramem systemowym oraz wewnętrznymi politykami Zamawiającego, a także po każdej zmianie w konfiguracji środowiska produkcyjnego. Mechanizmy synchronizacji powinny móc być uruchamiane nie rzadziej niż raz na godzinę.
13. Dostarczone rozwiązanie powinno umożliwiać selektywne testowanie każdej z aplikacji lub pojedynczych modułów dla każdej z wcześniejszych wersji bazy danych oraz aplikacji, przechowywanych w chmurze. Przez testowanie Zamawiający rozumie uruchomienie w chmurze w pełni działających aplikacji, zalogowanie się oraz skorzystanie z każdej dostępnej funkcjonalności. Architektura dostarczonego rozwiązania musi być oparta o serwery pośredniczące (proxy), tak by środowisko produkcyjne (lokalne) nie miało bezpośredniego dostępu do chmury, a chmura do środowiska lokalnego. Dotyczy to zarówno wymiany danych, jak również samej inicjacji połączeń między środowiskami.”
14. Rozwiązanie musi umożliwiać przepięcie użytkowników do aplikacji chmurowej w dwóch trybach:
    a. W przypadku niedostępności lokalnego systemu Asseco (np. zaszyfrowanie danych lokalnych przez ransomware, awarie serwerów, itp.), przy poprawnie działającej infrastrukturze lokalnej (sieci, stacje robocze, itp.) - przepięcie powinno odbywać się w sposób szybki i niezauważalny dla użytkowników, tj. brak zmian konfiguracyjnych na stacjach roboczych ani serwerach.

   b. W przypadku braku dostępności całej sieci lokalnej (sieci, serwery, itp.) – możliwe jest selektywne przepinanie wybranych stacji roboczych i użytkowników (tzw. szpital polowy).
15. Dla obu w/w scenariuszy użytkownicy powinni móc pracować na tych samych systemach co w środowisku lokalnym (w pełni odwzorowany zakres funkcjonalny oraz licencji).
16. Dostarczone rozwiązanie musi umożliwiać powrót do pracy w środowisku lokalnym po przywróceniu jego dostępności (synchronizacja wsteczna).
17. Architektura dostarczonego rozwiązania musi być oparta o serwery pośredniczące (proxy), tak by środowisko produkcyjne (lokalne) nie miało bezpośredniego dostępu do chmury, a chmura do środowiska lokalnego. Dotyczy to zarówno wymiany danych, jak również samej inicjacji połączeń między oboma środowiskami.
18. Rozwiązanie musi posiadać wbudowane mechanizmy ochrony przed ransomware, uniemożliwiające synchronizację do chmury danych, które zostały już zaszyfrowane w środowisku lokalnym lub proces szyfrowania jest w trakcie.
19. Komunikacja między środowiskiem lokalnym a chmurowym powinna być w pełni szyfrowana, zarówno na poziomie wymiany danych, jak również samej inicjacji połączeń.
20. Dostarczone rozwiązanie musi posiadać wbudowany panel administratora, umożliwiający realizację wszystkich kluczowych procesów.
21. Dostarczone rozwiązanie musi posiadać wbudowane narzędzia monitorowania i powiadamiania o przebiegu wszystkich kluczowych procesów i statusach pracy systemu, m.in. dostępność usług, statusów procesów synchronizacji danych, itp. Narzędzia monitorowania muszą udostępniać dashboardy graficzne, powiadomienia email, powiadomienia MS Teams.
22. Wykonawca zapewni utrzymywanie i serwisowanie całego środowiska przez okres trzech lat od podpisania umowy, w tym:
    a. wszystkie niezbędne licencje wymagane do tego rozwiązania,
    b. bieżące aktualizowanie wszystkich komponentów dostarczonego rozwiązania,
    c. wgrywanie poprawek bezpieczeństwa,
    d. monitorowanie poprawności działania oraz reagowanie na awarie w liczbie godzin nie przekraczającej 8h/ m-c,
    e. przeprowadzanie kompleksowych testów kopii chmurowych minimum raz w miesiącu,
    f. dostępność zespołu inżynierów dostarczonego rozwiązania oraz certyfikowanych inżynierów Oracle (lub równoważnego producenta baz danych).
23. W przypadku przełączenia szpitala na pracę w trybie Disaster Recovery Center (DRC) w środowisku chmurowym obowiązują następujące ograniczenia:
    a. Czas korzystania: możliwość pracy w trybie awaryjnym przez maksymalnie 45 dni roboczych.
    b. System AMMS: dostęp dla co najmniej 150 jednoczesnych sesji użytkowników.
    c. Systemy IM ERP oraz IM LAB: przy korzystaniu wyłącznie z licencji chmurowych – co najmniej 10 jednoczesnych sesji.
24. Rozwiązanie DRC stanowi środowisko awaryjne, które może być uruchamiane wyłącznie w przypadku wystąpienia poważnych lub krytycznych awarii, uniemożliwiających funkcjonowanie podstawowej infrastruktury Zamawiającego. Rozwiązanie to nie jest przeznaczone do obsługi planowych prac technicznych, krótkotrwałych przerw serwisowych ani jako narzędzie do bieżącego przełączania pracy pomiędzy środowiskami. DRC pełni rolę zabezpieczenia ciągłości działania szpitala wyłącznie w sytuacjach, gdy podstawowe środowisko produkcyjne staje się niedostępne i dalsze funkcjonowanie placówki byłoby zagrożone. Rozwiązanie DRC dla środowiska opartego o rozwiązania dostawcy ma być dostarczone w ramach Europejskiego

Obszaru Gospodarczego (EOG) w tzw. Suwerrenym Regionie i gwarantować wymagania suwerenności cyfrowej:

- Środowisko chmury obliczeniowej musi zapewnić, że wszystkie dane cyfrowe, w tym dane magazynowane i oprogramowanie, a także dane przesyłane przez sieci, są zgodne z przepisami prawa dotyczącymi suwerenności danych, w tym ogólnego rozporządzenia o ochronie danych (RODO), uchwalonego przez Unię Europejską w 2016 r.
- Środowisko musi znajdować się w całości na terytorium Unii Europejskiej (UE), być obsługiwane przez personel zamieszkały w UE i posiadać operatorów, którymi są podmioty prawne zarejestrowane w UE.
- Środowisko musi gwarantować wysoką dostępność w każdym regionie chmury, aby wspierać przywrócenie działania w przypadku awarii systemu w granicach danego kraju lub regionu.
- Środowisko musi być połączone z Internetem za pośrednictwem szyfrowanych łączy z zaawansowaną kontrolą dostępu. Klucze szyfrowania pozostają u Zamawiającego i nie są importowane do chmury. Dane przesyłane przez sieć (data in transit) muszą co najmniej korzystać z aktualnych protokołów zgodnych ze standardami takimi jak Transport Layer Security (TLS) 1.2 lub nowszymi oraz certyfikatami cyfrowymi X.509. Środowisko wykorzystywane przez Zamawiającego musi być odseparowane od danych innych klientów dostawcy usług
- Wymagane jest potwierdzenie weryfikacji działania według unijnego kodeksu postępowania w zakresie przetwarzania w chmurze - European Union (EU) Cloud Code of Conduct. Wymagania mogą zostać potwierdzone przez informacje zawarte na stronie internetowej dostawcy usług chmurowych.

25. W okresie obowiązywania trzyletniej umowy Dostawca gwarantuje Zamawiającemu możliwość maksymalnie trzykrotnego odtworzenia środowiska produkcyjnego z infrastruktury DRC do środowiska lokalnego:
    a. Koszty związane z przeprowadzeniem wskazanych trzech powrotów są w pełni uwzględnione w cenie usługi i nie powodują powstania dodatkowych zobowiązań finansowych po stronie Zamawiającego.
    b. Każdy kolejny powrót środowiska (powyżej przewidzianych trzech) realizowany będzie na podstawie odrębnych uzgodnień pomiędzy Stronami.
26. Dostarczenie usługi S3 Object Storage o pojemności maksimum 50 TB (wolumen przeznaczony wyłącznie na potrzeby kopii maszyn wirtualnych zgodnie z harmonogramem). Usługa ma być uzupełnieniem wyżej opisanego rozwiązania, umożliwiając dodatkowo cykliczne i automatyczne tworzenie kopii maszyn wirtualnych, wykorzystywanych w środowisku Zamawiającego, zgodnie z ustalonym harmonogramem, z zapewnieniem bezpieczeństwa i wysokiej dostępności. Usługa powinna spełniać następujące wymagania funkcjonalne:
    a. komunikacja z klientem realizowana poprzez protokół HTTPS, gwarantujący szyfrowane połączenie,
    b. dostęp do usługi zabezpieczony poprzez sekretny klucz i identyfikator usługi,
    c. dane przechowywane w repozytorium muszą być szyfrowane, przy użyciu klucza zarządzanego przez usługodawcę lub przy użyciu własnego klucza szyfrującego dostarczonego przez zamawiającego.
27. Dostarczenie modułu do składowania elektronicznej dokumentacji medycznej:

a. usługa umożliwia składowanie Elektronicznej Dokumentacji Medycznej poza infrastrukturą Zamawiającego, dając możliwość indeksowania i wymiany z innymi świadczeniodawcami za pomocą systemu P1,
b. podczas indeksacji dokumentów na platformie P1 jako repozytorium dokumentów, do którego po dokumenty mogą kierować się inni świadczeniodawcy i pacjenci, możliwe jest wskazanie repozytorium w usłudze chmurowej,
c. dostarczona usługa do komunikacji z systemem HIS musi wykorzystywać standard IHE (zgodnie z wytycznymi przygotowanymi do komunikacji z systemem P1),
d. dostawca skonfiguruje i uruchomi usługę do komunikacji z użytkowanym u świadczeniodawcy systemem HIS AMMS autorstwa Asseco Poland S.A.,
e. usługa musi umożliwiać przechowywanie w niej całości dokumentacji EDM wytwarzanej w jednostce lub tylko tej, która jest wymagana do indeksowania w ramach P1,
f. usługa dostarczana jest w modelu SaaS (Software as a Service),
g. możliwość składowania i udostępniania dokumentów wytworzonych w oparciu o standard HL7 CDA, w tym Polską Implementację Krajową (PIK) HL7 CDA,
h. w celu zapewnienia wysokiego poziomu bezpieczeństwa Dostawca zapewni objęcie usługi monitoringiem prowadzonym przez Security Operation Center (SOC) działającym w trybie 24/7/365,
i. dokumenty w ramach usługi przechowywane są na terenie Rzeczypospolitej Polskiej. Dostawca zobowiązany jest wskazać lokalizację Centrów Przetwarzania Danych wykorzystywanych na potrzeby usługi,
j. dostawca dostarczy komplet dokumentów opisujących szczegółowo zasady korzystania z usługi z uwzględnieniem wymagań RODO (w tym Regulamin, Opis usługi, Umowę Powierzenia Przetwarzania Danych),
k. każdy dokument przed zapisem musi zostać zweryfikowany systemem antywirusowym,
l. każdy dokument przed zapisem musi zostać zaszyfrowany,
m. składowanie dokumentów oraz możliwość rozbudowy w wymiarze 60 GB przestrzeni i do 25 tys. dokumentów miesięcznie (podany wolumen dotyczy wyłącznie bieżącego składowania nowych dokumentów),
n. usługa dostępna będzie przez 36 miesięcy od daty jej uruchomienia,
o. w ramach usługi Dostawca zapewni kopie zapasowe danych z minimum 3 dni wstecz,
p. dostawca zapewni wysoki poziom bezpieczeństwa dla komunikacji pomiędzy usługą a infrastrukturą Zamawiającego. W przypadku wykorzystania komunikacji SSL w ramach usługi Wykonawca dostarczy niezbędne certyfikaty WSS, TLS,
q. zgłoszenie błędów możliwe będzie telefonicznie, drogą elektroniczną z wykorzystaniem poczty email lub dedykowanego portalu umożliwiającego zgłoszenie. Błędy klasyfikowane będą w jednej z dwóch kategorii:
   - Błąd krytyczny - sytuacja, w której niemożliwie jest użytkowanie Oprogramowania Aplikacyjnego w zakresie jego Podstawowej Funkcjonalności (t.j. takiej, która dotyczy każdego użytkownika, występuje na każdej Stacji roboczej skonfigurowanej do pracy z Oprogramowaniem Aplikacyjnym zgodnie z zaleceniami producenta Oprogramowania Aplikacyjnego w tym na każdej przeglądarce zalecanej i skonfigurowanej do pracy z Oprogramowaniem Aplikacyjnym zgodnie z zaleceniami producenta) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego. Czas reakcji 1 dzień roboczy z wyłączeniem dni ustawowo wolnych od pracy, czas naprawy do 3 dni roboczych

- Błąd zwykły - niespowodowane przez użytkownika, niezgodne z dokumentacją, powtarzalne działanie Oprogramowania Aplikacyjnego, występujące w tym samym miejscu programu, na stacji roboczej skonfigurowanej zgodnie z zaleceniami producenta Oprogramowania Aplikacyjnego i prowadzące w każdym przypadku do otrzymania błędnych wyników jego działania, udokumentowane co najmniej poprzez opis ścieżki powtórzenia, zapisy logów systemowych i/lub zrzuty ekranów. Wszelkie uwagi związane z wyglądem, estetyką, ergonomią bądź przyzwyczajeniami Użytkownika (Zamawiającego) oraz uwagi dotyczące rozbudowy lub ograniczenia funkcjonalności nie są traktowane jako Błędy. Czas reakcji 15 dni roboczych z wyłączeniem dni ustawowo wolnych od pracy, czas naprawy do 60 dni roboczych

r. czas naprawy- czas liczony od momentu podjęcia przez wykonawcę działań mających na celu usunięcie Błędu do momentu jego usunięcia przez Wykonawcę
s. przerwy techniczne w ciągu miesiąca kalendarzowego nie mogą trwać dłużej niż 48 godzin i nie powinny rozpoczynać się przed godziną 19:00,
t. o planowanych przerwach technicznych Wykonawca zobowiązany jest informować Zamawiającego z minimum 2 dniowym wyprzedzeniem,
u. w przypadku rezygnacji przez Zamawiającego z usługi Dostawca przekaże całość zdeponowanej w usłudze dokumentacji w formacie umożliwiającym zaimportowanie dokumentów,

28. Zamawiający wymaga dostarczenia niezbędnych licencji, umożliwiających instalację oraz uruchamianie w/w systemów Asseco w chmurze, tj. HIS, LIS oraz ERP, w tym zapewnienie odpowiednich licencji chmurowych producenta oprogramowania (licencji na kopię AMMS w chmurze). Wymóg dostarczenia licencji dotyczy zarówno części obligatoryjnej jak i części dodatkowej opisanej w pkt 27 (w sytuacji zaoferowania dodatkowych funkcjonalności).

Pkt 27 opisuje funkcjonalności dodatkowe, niewymagane w podstawowym zakresie zadania 2 (części 2)

Wymaganie dotyczące oprogramowania bazodanowego:

Wykonawca dostarczy i wdroży oprogramowanie bazodanowe Oracle Standard Edition 2. Ponadto Wykonawca dokona procesu reinstalacji (migracji) baz danych z posiadanej przez Zamawiającego wersji (wydania) do oferowanej wersji (wydania) kompatybilnej z posiadanym przez Zamawiającego oprogramowaniem (w szczególności klasy HIS) oraz wymaganiami oferowanego rozwiązania chmurowego. Migracja dotyczy baz danych takich jak: HIS, ERP, MPI, EDM

W ramach procesu migracji Wykonawca jest zobowiązany do wykonania następujących zadań:

a) Wykonania audytu bieżącej instalacji baz danych celem określenia szczegółowej listy elementów niestandardowych, które będą podlegały odtworzeniu na nowym środowisku baz danych w szczególności użytkowników systemowych oraz bazodanowych, skryptów automatyzujących pracę bazy danych, itp.
b) Przedstawienia planu (w tym harmonogramu) reinstalacji do akceptacji Zamawiającego
c) Wykonawca przed rozpoczęciem migracji wykona pełną kopię bezpieczeństwa baz danych i przekaże Zamawiającemu raport z ich integralności;
d) Wykonania zaakceptowanego planu migracji baz danych oraz weryfikacji działania
e) Przeszkolenia administratorów Zamawiającego z nowej konfiguracji baz danych.
f) Wykonania testów potwierdzających poprawne funkcjonowanie baz danych.
g) Wykonania kopii zapasowych systemów bazodanowych
h) Przygotowanie procedury rollback (powrotu) obejmujące przygotowanie planu awaryjnego (rollback plan) na wypadek niepowodzenia migracji.

Wymagania dotyczące oprogramowania bazodanowego:

Możliwość instalacji oprogramowania na serwerach o pojemności socketów CPU nie przekraczającej 2.

1. Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (Solaris dla procesorów SPARC, IBM AIX dla procesorów POWER, Intel/AMD Linux, MS Windows). Identyczna funkcjonalność serwera bazy danych na ww. platformach.

2. Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, etc. Licencje nie mogą być ograniczone czasowo. Licencje nie mogą zawierać ograniczeń co do stosowania aplikacji wyłącznie wskazanego (nazwanego) producenta (wymagane są licencje tzw. full use).

3. Proponowany zestaw licencji powinien być jednorodny. Wymagana jest dostawa oprogramowania certyfikowanego pod względem zgodności ze sobą. Wymaganie obejmuje:

a) Oprogramowanie bazy danych ze względu na zgodność z systemem operacyjnym oraz platformą sprzętową,

b) Systemy operacyjne używane do uruchamiania serwerów bazy danych ze względu na zgodność z platformą sprzętową.

4. Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu).

5. Oprogramowanie klienckie, za pomocą którego można łączyć się do bazy danych musi być dostępne na wielu platformach systemowo-sprzętowych (minimalny zakres platform taki jak dla oprogramowania serwera bazy danych)

6. Wsparcie protokołu XA.

7. Wsparcie standardu JDBC 3.0.

8. Zgodność ze standardem ANSI/ISO SQL 2016 lub nowszym.

9 .Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.

10. RDBMS musi zapewniać niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych.

11. RDBMS musi zapewniać przetwarzanie transakcyjne wg reguł ACID z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji musi pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, spójny odczyt nie może blokować możliwości wykonywania zmian.

12. RDBMS musi posiadać możliwość zagnieżdżania transakcji – możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej.

13. Dostępność nieblokującego poziomu izolowania transakcji „tylko do odczytu” (Read Only) pozwalający na uzyskanie w wielu kolejnych następujących po sobie zapytaniach rezultatów odzwierciedlających stan danych z chwili rozpoczęcia ww. transakcji.

14. Dostępność poziomu serializowanego poziomu izolowania transakcji (Serializable).

15. Możliwość zmiany domyślnego trybu izolowania transakcji (Read Commited) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych.

16. Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode) zarówno po stronie serwera bazy danych jak i oprogramowania klienckiego. Wsparcie dla polskich stron kodowych – ISO-8859-2, MS Windows Code Page 1250 oraz PC 852. Automatyczna konwersja znaków pomiędzy różnymi ustawieniami stron kodowych po stronie klienta i serwera bazy danych.

17. Możliwość migracji bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode.

18. Możliwość definiowania w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku.

19 Możliwość bez dodatkowych ograniczeń przechowywania wierszy, których rozmiar przekracza rozmiar bloku bazy danych.

20. Możliwość budowania indeksów o strukturze B-drzewa. Baza danych powinna umożliwiać założenie indeksu jednej lub większej liczbie kolumn tabeli, przy czym ograniczenie liczby kolumn na których założony jest 1 indeks nie powinno być mniejsze niż 16.

21. Możliwość budowania widoków zmaterializowanych odzwierciedlających stan danych zdefiniowanych przez zapytanie SQL. Widok zmaterializowany przechowuje rezultat zapytania, którego aktualizacja odbywa się w jednej z dostępnych strategii – na żądanie, okresowo bądź po każdym zatwierdzeniu transakcji modyfikującej tabele, na której oparty jest widok zmaterializowany.

22. Możliwość szybkiego odświeżania danych w widoku zmaterializowanym na podstawie mechanizmu identyfikacji zmian w danych źródłowych.

23. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).

24. Kosztowy model optymalizacji instrukcji SQL.

25. Model statystyk optymalizatora kosztowego musi pozwalać na odwzorowanie nierównomierności rozkładu danych (składowanie informacji o rozkładzie wartości występujących w kolumnach za pomocą histogramu bądź porównywalnego funkcjonalnie modelu odwzorowania).

26. Możliwość uwzględnienia korelacji wartości występujących w niezależnych kolumnach tabeli w modelu statystyk optymalizatora kosztowego.

27. RDBMS powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.

28. 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.

29. Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).

30. Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej).

31. 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 DML, 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).

32. 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.

33. Możliwość wykonania równoczesnych operacji DML (Insert/Update/Delete) na tej samej tabeli .

34. Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu zewnętrznego w stosunku do bazy danych.

35. 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.

36. 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, itp.). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online(hot backup)..

37. 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.

38. Możliwość uruchomienia bazy danych w środowisku klastra serwerów bazy danych w trybie HA (High-avalability) przy pomocy dostarczanego przez dostawcę modułu zarządzającego bazą danych w klastrze.

39. Możliwość przeniesienia bazy danych pracującej na jednym z serwerów klastra na inny serwer klastra np. z powodu przeprowadzania czynności utrzymaniowych.

40. Każdy z serwerów klastra musi mieć możliwość uspójnienia lub odtworzenia całej bazy danych w sytuacji awarii nośników lub nagłego zatrzymania innego serwera.

41. Dostarczone licencje muszą umożliwiać pracę z dowolną aplikacją, bądź oprogramowaniem narzędziowym

42. Liczba dostarczonych licencji - 2 szt.

43. Wraz z licencją dostarczone ma być wsparcie realizowane przez producenta oprogramowania na okres 12 miesięcy (Software Update License & Support). Dodatkowo wsparcie może być wydłużone do 36 miesięcy.