

Załącznik nr 5i do SIWZ

Wdrożenie systemu oraz asysta techniczna

Prze przystąpieniem do prac Wykonawca opracuje i uzgodni z Zamawiającym oraz Inżynierem Kontraktu szczegółowy plan wdrożenia co najmniej w następującym zakresie:

1. Harmonogram wdrożenia w zakresie systemów informatycznych oraz infrastruktury technicznej.
2. Analizę przedwdrożeniową w zakresie dostarczanej infrastruktury technicznej w zakresie zakładanej konfiguracji, parametryzacji oraz podłączenia z istniejącą u Zamawiającego infrastrukturą techniczną.
3. Analizę przedwdrożeniową zawierającą szczegółowy opis funkcjonalności systemów informatycznych objętych wdrożeniem wraz z przedstawieniem wyglądu formularzy i przedstawieniem sposobu realizacji wymaganych w SIWZ funkcjonalności systemów informatycznych.
4. Plan testów wdrażanych systemów informatycznych z przypadkami użycia.
5. Plan szkoleń użytkowników oraz dokumentację szkoleniową.

Wdrożenie obejmować będzie instalację i konfigurację oprogramowania na serwerze: dostawę licencji i udzielenie licencji na czas nieokreślony, instalację i konfigurację, przygotowanie serwera/ów.

Po zakończeniu wdrożenia Wykonawca opracuje i uzgodni z Zamawiającym oraz Inżynierem Kontraktu dokumentację powdrożeniową obejmującą co najmniej:

1. Dokumentację powdrożeniową dostarczonej infrastruktury technicznej zawierającej szczegółową konfigurację, adresację, nazewnictwo elementów infrastruktury, powiązania z istniejącą przed wdrożeniem infrastrukturą techniczną.
2. Dokumentację powdrożeniową dostarczonych systemów informatycznych dla użytkownika, instruktora oraz administratora systemów.
3. Instrukcję eksploatacji w zakresie wszystkich dostarczonych elementów infrastruktury technicznej.
4. Instrukcję eksploatacji w zakresie wszystkich dostarczonych systemów informatycznych.

Szkolenia użytkowników

- Do każdego modułu wspomagającego obsługę obszarów działalności urzędu, Zamawiający wskaże osoby, które zostaną przeszkolone.
- Zamawiający wymaga przeprowadzenia maksymalnie 50 roboczodni szkoleń, przy czym wszystkie osoby wskazane do szkoleń przez Zamawiającego mają zostać przeszkolone w stopniu umożliwiającym im samodzielną pracę z systemem.
- Szkolenia będą realizowane w pomieszczeniach i na sprzęcie udostępnionym przez urząd.
- Nie przewiduje się przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych.
- Dopuszcza się po uzgodnieniu z Zamawiającym przeprowadzenie szkoleń grupowych w wybranych obszarach tematycznych.

W ramach usługi zostaną zrealizowane szkolenia administratorów (1 administrator) i użytkowników (łącznie 20 użytkowników):

1. zakres szkoleń dla administratorów:
 - a. koncepcja i działanie wdrażanego systemu,
 - b. szczegółowa architektura rozwiązania,



- c. integracja z innymi systemami,
 - d. sposób instalacji systemu,
 - e. sposób instalacji nowych wersji systemu oraz poprawek do systemu,
 - f. monitorowanie poszczególnych warstw architektury: aplikacje, bazy danych, systemy operacyjne,
 - g. budowa widoków,
 - h. analiza historyczna zebranych danych,
 - i. tworzenie raportów i analiz,
 - j. interfejs graficzny poszczególnych modułów systemu,
 - k. możliwości rozszerzenia i rozwoju,
 - l. obsługa serwisowa systemu.
2. zakres szkoleń dla użytkowników:
 - a. interfejs graficzny systemu,
 - b. szczegółowe funkcjonalności wybranych modułów systemu,
 - c. szczegółowy instruktaż stanowiskowy,
 - d. tworzenie raportów i analiz,
 - e. zgłaszanie błędów i usterek w działaniu systemu.

Szkolenia zostaną przeprowadzone w pomieszczeniach udostępnionych przez Zamawiającego.

Asysta techniczna

Usługi asysty technicznej mają ułatwić pracę użytkownikom systemu i zapewnić prawidłowe działanie systemu pod względem funkcjonalnym i jakościowym w okresie trwania projektu. Usługi asysty technicznej obejmować będą:

- a) świadczenie pomocy technicznej typu „HELP DESK”,
- b) świadczenie usług utrzymania i konserwacji dla dostarczonego oprogramowania,
- c) dostarczanie nowych wersji oprogramowania będących wynikiem wprowadzenia koniecznych zmian w funkcjonowaniu systemu związanych z wejściem w życie nowych przepisów,
- d) przekazywanie w terminach uprzedzających datę wejścia w życie znowelizowanych lub nowych przepisów prawa nowych wersji oprogramowania, włącznie z koniecznym w tym zakresie udzieleniem licencji do nowej wersji systemu,
- e) dostarczanie nowych, ulepszonych wersji oprogramowania lub innych komponentów systemu będących konsekwencją wykonywania w nich zmian wynikłych ze stwierdzonych niedoskonałości technicznych,
- f) zdalną instalację nowych wersji oprogramowania i aktualizacji bibliotek oprogramowania,
- g) dostarczanie nowych wersji dokumentacji użytkownika oraz dokumentacji technicznej zgodnych co do wersji jak i również zakresu zaimplementowanych i działających funkcji z wersją dostarczonego oprogramowania aplikacyjnego,
- h) świadczenie telefonicznie usług doradztwa i opieki w zakresie eksploatacji systemu lub na miejscu, jeżeli wymagają tego kwestie techniczne lub organizacyjne, a nie jest to spowodowane brakiem wiedzy lub przeszkolenia pracowników, a brak podjęcia takiego działania przez Wykonawcę może spowodować nieprawidłową eksploatację systemu lub czasowe jej wstrzymanie,
- i) podejmowanie czynności związanych z diagnozowaniem problemów oraz usuwaniem przyczyn nieprawidłowego funkcjonowania dostarczonego rozwiązania z wykorzystaniem zdalnego dostępu przez tunelowane połączenie typu VPN lub innego bezpiecznego, zdalnego dostępu do infrastruktury teleinformatycznej.
- j) Zamawiający wymaga 60-miesięcznego okresu asysty technicznej.
- k) asysta techniczna jak i gwarancja mogą być świadczone w sposób zdalny, w szczególności za pomocą uzgodnionego z Zamawiającym oprogramowania typu VPN.



Gwarancja

1. Zamawiający wymaga co najmniej 60-miesięcznego okresu gwarancji.
2. Gwarancja udzielana przez Wykonawcę obejmuje usuwanie wszelkich wad i usterek wykrytych przez użytkowników Zamawiającego uniemożliwiających wykorzystywanie funkcji systemu, przy czym:
 - a. awaria rozumiana jest jako niepoprawne działanie oprogramowania, które uniemożliwia prawidłową eksploatację systemu i powoduje konieczność wstrzymania jego eksploatacji,
 - b. usterka to nieprawidłowe lub niezgodne z dokumentacją wykonywanie funkcji systemu, niepowodujące jednak konieczności wstrzymania eksploatacji systemu.
3. W ramach gwarancji Wykonawca zobowiązuje się do utrzymywania zgodności systemu z wymaganiami prawa.

Oprogramowanie systemowe i bazodanowe na potrzeby Zintegrowanego Systemu Finansowo – Księgowego

W ramach projektu nastąpi dostawa, instalacja, konfiguracja, testowanie i uruchomienie oprogramowania systemowego i bazodanowego na serwerze zakupionym w ramach projektu. Oprogramowanie systemowe i bazodanowe ma zostać wykorzystane przez zaoferowane w ramach projektu systemy.

1. Zakup oprogramowania systemowego (OS) o następującym minimalnym zakresie funkcjonalnym:
 - a) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń przychodzących i wychodzących;
 - b) Możliwość uruchomienia systemu w trybie tekstowym lub graficznym;
 - c) Obsługa systemów wieloprocesorowych 64 rdzeniowych;
 - d) Obsługa platform sprzętowych x86, x64
 - e) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania wszystkich składników systemu bez wykonania żadnego restartu systemu operacyjnego. Brak konieczności restartu systemu operacyjnego;
 - f) Możliwość uruchomienia nieograniczonej ilości wirtualnych instancji na serwerze. Wiele systemów operacyjnych, wiele wersji, różne konfiguracje wydajności i bezpieczeństwa - wszystko uruchomione jednocześnie na tym samym fizycznym serwerze;
 - g) Możliwość wirtualizacji pamięci masowej. Pozwala wielu wirtualnym systemom uruchomionym na tym samym lub różnych serwerach na dostęp do współdzielonej pamięci masowej lub systemu plików. Wirtualizacja pamięci masowej pozwala w pełni wykorzystać zalety wirtualizacji;
 - h) Możliwość zastosowania para-wirtualizacji dla wszystkich urządzeń systemu operacyjnego.
2. Zakup oprogramowania serwera aplikacji (AS) o następującym minimalnym zakresie funkcjonalnym:
 - a) Wymagania odnośnie standardów jakie musi spełniać infrastruktura serwera aplikacji
 - b) Wymagania odnośnie obsługi standardów bezpieczeństwa, jakie musi spełniać infrastruktura serwera aplikacji.
 - c) Infrastruktura serwera aplikacji musi posiadać możliwość realizacji odpowiedniego poziomu bezpieczeństwa w zakresie:
 - Uwierzytelniania
 - kontroli dostępu
 - zarządzania użytkownikami, grupami i rolami
 - tworzenia, przechowywania i walidacji certyfikatów, haseł, kluczy
 - audytowania zdarzeń bezpieczeństwa

- wsparcia dla mechanizmu pojedynczego logowania SSO
 - d) 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
 - e) 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
 - f) 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)
 - g) 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.
 - h) Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę standardów SAML 1.1, SAML 2.0 lub wyższych
 - i) 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)
 - j) Infrastruktura serwera aplikacji musi posiadać wbudowane API do funkcjonalności przeszukiwania i walidacji certyfikatów X.509 (CLV – Certificate Lookup and Validation)
 - k) Infrastruktura serwera aplikacji musi posiadać obsługę mechanizmów autoryzacji i mapowania ról przy użyciu standardu XACML 2.0
 - l) Infrastruktura serwera aplikacji musi posiadać wbudowaną obsługę protokołu SNMP v3 wraz z HMAC-MD5-96, HMAC-SHA-96
 - m) Oprogramowanie musi być objęte licencją dożywotnią.
 - n) Dostarczona licencja musi być typu „na procesor/rdzeń procesora”.
 - o) Dostarczone licencje nie mogą mieć ograniczeń użytkowników i muszą zapewniać Nielimitowane połączenie do bazy.
3. Zakup oprogramowania bazodanowego (DB) o następującym minimalnym zakresie funkcjonalnym:
- a) Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów PA-RISC i Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX), Intel/AMD Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach.
 - b) Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych.
 - c) Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności migracji środowiska aplikacyjnego.
 - d) Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. 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 przeglądanych zbioru danych.
 - e) Możliwość zagnieżdżenia transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.

- f) Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
- g) Możliwość migracji zestawu znaków bazy danych do Unicode
- h) Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
- i) Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych
- j) Możliwość utworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych
- k) Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
- l) Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych
- m) 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.
- n) 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.
- o) 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. Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online
- p) Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup).
- q) 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.
- r) W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników.
- s) Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.
- t) Możliwość oddzielenia w ramach silnika bazy danych instancji odpowiedzialnej za obsługę danych oraz za rozmieszczenie danych na dyskach jako dwa odrębne byty osobno administrowane.
- u) Umożliwia wydzielenie osobnej podsieci do komunikacji pomiędzy instancjami odpowiedzialnymi za rozmieszczenie danych na dyskach.
- v) Możliwość zastosowania natywnych filtrów dostępnych z poziomu oprogramowania bazodanowego które zapewnią, że do urządzeń dyskowych wykorzystywanych w ramach instancji bazy danych nie będą wysyłane żadne instrukcje poza tymi które są autoryzowane przez bazę danych.
- w) Oprogramowanie musi być objęte licencją dożywotnią.
- x) Dostarczona licencja musi być typu „na procesor/rdzeń procesora”. Dostarczone licencje nie mogą mieć ograniczeń użytkowników i muszą zapewniać Nielimitowane połączenie do bazy
- y) warunki serwisu gwarancyjnego – co najmniej 24 miesiące.

