

**WYMAGANIA TECHNICZNE I NIEFUNKCJONALNE
APLIKACJI PŁACOWEJ DLA FUNKCJONARIUSZY SOP
PODLEGAJĄCE NEGOCJACJOM**

I. WYMAGANIA TECHNICZNE

WYMAGANIA ZAMAWIAJĄCEGO	
Lp.	Wymagania techniczne dla aplikacji
1	Licencjonowanie
1.1	Rodzaj licencji – dożywotnia na wskazaną w punkcie 2.3.3 liczbę użytkowników dla wymaganych przez Zamawiającego funkcjonalności.
1.2	Zamawiający nie wymaga od Wykonawcy przeniesienia na niego autorskich praw majątkowych dla aplikacji będącej przedmiotem zamówienia.
1.3	Zamawiający dopuszcza wykorzystanie do budowy aplikacji komponenty oprogramowania otwartego (ang. Open Source). Przeniesienie autorskich praw majątkowych do komponentów oprogramowania otwartego, stanowiących składową dostarczonej aplikacji, licencjonowanych w trybie GNU GPL jest wyłączone.
2	Wymagania dla aplikacji
2.1	Wydajność
2.1.1	Czas pobierania danych do pojedynczego formularza z bazy danych za pomocą interfejsu użytkownika – max. 10 sekund.
2.1.2	Czas zapisu danych z pojedynczego formularza do bazy danych za pomocą interfejsu użytkownika – max. 10 sekund.
2.1.3	Czas wygenerowania prostego raportu – max. 2 minuty
2.1.4	Czas wygenerowania największego raportu – max. 10 minut
2.2	Architektura logiczna i fizyczna/Niezawodność
2.2.1	Aplikacja musi być tak zaprojektowana (konfiguracja programowa, procedury odtwarzania po awarii, konfiguracja sprzętowa), aby w ciągu max. 8 godzin Administrator mógł przywrócić wszystkie dane przetwarzane i przechowywane przez aplikację oraz jej konfigurację z kopii zapasowej.
2.3	Architektura systemu

2.3.1	Aplikacja musi być tak zaprojektowana, aby działała w architekturze klient-serwer. Aplikacja działająca po stronie serwera musi pracować pod kontrolą systemu operacyjnego z rodziny Microsoft Windows Server. Aplikacja dla klienta musi pracować pod kontrolą systemu operacyjnego minimum Windows 10 Professional zarówno w wersjach 32-bitowej jak i 64-bitowej lub nowszego.
2.3.2	Interfejs użytkownika – Zamawiający wymaga dla aplikacji serwera oraz klienta środowiska działającego w trybie graficznym, dla systemu operacyjnego wymienionego w pkt. 2.3.1. Nie dopuszcza się zastosowania środowiska tekstowego oraz wiersza poleceń dla interfejsów użytkownika.
2.3.3	Aplikacja musi być przeznaczona wydajnościowo dla min. 50 użytkowników (aplikacja musi stworzyć możliwość pracy przez min. 50 użytkowników, bez dokonywania w nim jakichkolwiek zmian i modyfikacji). W momencie wdrożenia wymagana będzie dostawa licencji na 15 równocześnie pracujących użytkowników (oznacza to, że w aplikacji może być założonych więcej niż 15 użytkowników, natomiast max. tylko 15 użytkowników może pracować równocześnie) - nie dotyczy kont Administratorów. Liczba kont o uprawnieniach Administratorów nie jest wliczana do liczby licencji dla kont o uprawnieniach użytkownika.
2.4	Identyfikacja/Uwierzytelnianie
2.4.1	<p>Identyfikacja i uwierzytelnianie realizowane są poprzez: podanie unikalnego identyfikatora użytkownika (login) oraz hasła użytkownika. Mechanizm logowania musi umożliwiać min. jedno z następujących źródeł identyfikatorów użytkowników:</p> <ol style="list-style-type: none"> 1. przechowywanie loginów i haseł wewnątrz aplikacji - w obiekcie niezależnym od systemu operacyjnego (Złożoność hasła oraz jego długość muszą być konfigurowalne. Hasła w bazie danych użytkowników nie mogą być przechowywane w postaci jawnej (dopuszcza się funkcje skrótu inne niż MD5 - preferowane SHA-2)). 2. integrację z Active Directory – nazwy użytkowników i hasła użytkowników przechowywane w Active Directory (Aplikacja może jedynie odczytywać atrybuty obiektów z Active Directory).
2.5	Autoryzacja

2.5.1	Mechanizm autoryzacji musi jednoznacznie wskazywać, jakie operacje może wykonać użytkownik. Autoryzacja działań użytkownika ostatecznie odbywa się przy próbie inicjalizacji dostępu podmiotu do obiektu w systemie. Nadawanie uprawnień do operacji musi być realizowane w oparciu o grupy uprawnień.
2.6	Audyt/Rozliczalność
2.6.1	Aplikacja musi zawierać mechanizm zapewniający audyt działań wykonywanych przez użytkowników w systemie. Zakres mechanizmu audytu musi zapewniać rozliczalność użytkowników z punktu widzenia dostępu ich do obiektów (odczyt, zapis, modyfikacja, usunięcie) oraz modyfikacji uprawnień dostępu do tych obiektów w aplikacji. Mechanizm ten musi funkcjonować od momentu identyfikacji podmiotu – nawet, jeśli jego uwierzytelnienie się nie powiodło.
2.6.2	Każdy wpis w dzienniku zdarzeń systemu musi zawierać minimalnie następujące pola: <ul style="list-style-type: none"> ▪ auto numer Id; ▪ data (rok-miesiąc-dzień w formacie RRRR-MM-DD) i czas (godzina, minuta, sekunda w formacie GG.MM.SS) wystąpienia zdarzenia; ▪ identyfikator użytkownika; ▪ kod zdarzenia jednoznacznie identyfikujący działanie; ▪ parametry dla wykonywanej operacji, o ile są dostępne;
2.6.3	Mechanizm audytu oraz przechowywane w wyniku jego działania logi muszą być dostępne niezależnie od ponownego uruchomienia aplikacji lub systemu operacyjnego w bazie danych.
2.7	Budowa aplikacji
2.7.1	Aplikacja musi mieć budowę modułową. Każdy moduł składa się z jednej lub wielu funkcji. Użytkownicy muszą być organizowani w grupy użytkowników pełniących te same role w systemie. Dla każdej grupy użytkowników określony jest dostęp do modułów na podstawie przynależności do grupy użytkowników.
2.7.2	Aplikacja musi posiadać min. 2 moduły: <ul style="list-style-type: none"> • Administracyjny – realizujący minimum wszystkie wymagania opisane w punkcie 2.9.

	<ul style="list-style-type: none"> • Kadrowo kadrowo-płacowy – realizujący wszystkie cechy funkcjonalne opisane w Części I „WYMAGANIA FUNKCJONALNE APLIKACJI PŁACOWEJ DLA SOP DLA OBSŁUGI FUNKCJONARIUSZY”.
2.9	Wymagania dla modułu administracyjnego
2.9.1	Moduł administracyjny jest modułem wbudowanym w aplikację.
2.9.2	Do modułu „ <i>administracyjnego</i> ” przypisany na stałe dostęp wyłącznie dla grupy użytkowników wbudowanych „ <i>Administratorzy</i> ”.
2.9.3	<p>Funkcje w ramach modułu są organizowane w grupy następujących funkcji:</p> <ul style="list-style-type: none"> ▪ Ustawiające parametry globalne systemu, dostępne wyłącznie dla grupy wbudowanej „<i>Administratorzy</i>”. ▪ Zarządzające kontami użytkowników, grupami użytkowników oraz uprawnieniami grup użytkowników do modułów, dostępne wyłącznie dla grupy wbudowanej „<i>Administratorzy</i>”;
2.9.4	<p>Grupa funkcji „<i>Parametry globalne systemu</i>” to funkcje ustawiające/definiujące minimum następujące parametry:</p> <ul style="list-style-type: none"> ▪ definiowanie złożoności hasła użytkownika (dla mechanizmu przechowywania loginów i haseł wewnątrz aplikacji): definiowanie minimalnej długości hasła, złożoności i struktury hasła (z jakich znaków ma się składać), ilości prób nieprawidłowego zalogowania, po których konto się blokuje. ▪ liczbę nieudanych prób logowania wymagana do zablokowania konta. (przypadku zablokowania konta użytkownika standardowego w aplikacji konto w Active Directory nie zostaje zablokowane).
2.9.5	<p>Grupa funkcji „<i>Zarządzające kontami użytkowników, grupami użytkowników oraz uprawnieniami grup użytkowników</i>” to funkcje umożliwiające minimum:</p> <ol style="list-style-type: none"> 1. dodanie konta użytkownika; 2. usunięcie konta użytkownika; 3. modyfikacja ustawień konta użytkownika (modyfikowalne wszystkie parametry, oprócz nazwy konta); 4. odblokowanie konta użytkownika; 5. wyłączenie/włączenie konta użytkownika; 6. przypisanie użytkownika do określonej grupy użytkowników;

	<ol style="list-style-type: none"> 7. usunięcie użytkownika z określonej grupy użytkowników; 8. podgląd informacji do jakiej grupy/grup jest użytkownik przypisany; 9. ustawienie nowego hasła użytkownika z koniecznością jego zmiany przy pierwszym logowaniu; 10. podgląd aktualnie zalogowanych użytkowników; 11. dodanie/usunięcie dla grupy użytkowników dostępu do modułów; 12. wyświetlenie dziennika zdarzeń z możliwością sortowania oraz filtrowania (wpisywanie maski) po wszystkich dostępnych kolumnach; 13. export wyświetlonego dziennika zdarzeń do zewnętrznego pliku (min. plik w formatach : txt, csv, xml); 14. czyszczenie dziennika zdarzeń ze wszystkich pozycji z jednoczesnym zapisem wykonania tej operacji w dzienniku.
2.9.8	<p>Minimalne parametry konta użytkownika:</p> <ul style="list-style-type: none"> ▪ login (nazwa użytkownika); ▪ hasło w aplikacji nie może być przechowywane w postaci jawnej. Musi być zaszyfrowane lub być wpisane jako efekt działania funkcji skrótu (nie dopuszcza się funkcji skrótu MD5-preferowane SHA-2), ▪ stan blokady konta. Dopuszczalne stany: aktywne/nieaktywne – W przypadku stanu konta: „aktywne” użytkownik może zalogować się do systemu, w przeciwnym wypadku użytkownik nie może się zalogować do systemu. ▪ stan włączenia konta: Dopuszczalne stany: włączone/wyłączone – W przypadku stanu konta: „włączone” użytkownik może zalogować się do systemu, w przeciwnym wypadku użytkownik nie może się zalogować do systemu. ▪ „zmień hasło przy logowaniu” – atrybut wymaga zmiany hasła przy logowaniu – nie dotyczy kont importowanych z Active Directory.
2.9.9	<p>W aplikacji muszą być zaimplementowane następujące mechanizmy dotyczące kont użytkowników:</p> <ul style="list-style-type: none"> ▪ konto blokuje się po zdefiniowanej globalnie (jako parametr główny systemu) liczbie nieudanych prób logowania do aplikacji. Konto zablokowane uniemożliwia zalogowanie od aplikacji.

	<ul style="list-style-type: none"> ▪ wyłączenie konta w aplikacji powoduje automatyczne wykasowanie sesji użytkownika, a co się z tym wiąże – automatyczne wylogowanie użytkownika z aplikacji. ▪ jeśli użytkownikowi zaznaczono opcję „Zmień hasło podczas logowania” to musi on podać 2 razy identyczne hasło.
3	Procedury administracyjne
3.1	Aplikacja musi mieć możliwość wykonania kopii zapasowej konfiguracji aplikacji oraz pełnej kopii zapasowej danych przez nią przetwarzanych i w niej przechowywanych za pomocą mechanizmu przygotowanego przez Wykonawcę.
3.2	Aplikacja musi mieć możliwość odzyskania z kopii zapasowej konfiguracji aplikacji oraz wszystkich danych przetwarzanych i przechowywanych przez aplikację z kopii zapasowej danych za pomocą mechanizmu przygotowanego przez Wykonawcę.
3.3	Dla czynności określonych w pkt. 3.1 oraz 3.2 Wykonawca przygotowuje procedury w postaci dokumentów w języku polskim.