Tytuł:Autoryzacja (Login / Rejestracja / Wylogowanie)

Rozszerzona User Story (opis funkcjonalności)

Jako użytkownik chcę mieć możliwość założenia konta, aby uzyskać dostęp do wszystkich funkcji aplikacji, takich jak edytor tekstu, kalendarz czy lista zadań. Proces rejestracji powinien być prosty i przejrzysty — wystarczy adres e-mail oraz hasło, które spełnia podstawowe wymogi bezpieczeństwa (np. długość, znaki specjalne). Po poprawnej rejestracji użytkownik powinien zostać automatycznie zalogowany lub przekierowany do ekranu logowania.

Po założeniu konta użytkownik powinien mieć możliwość zalogowania się przy użyciu zarejestrowanego adresu e-mail i hasła. System powinien informować o błędach, np. nieprawidłowym haśle, braku konta lub zablokowanym użytkowniku. Sesja użytkownika powinna być bezpieczna i wygodna — np. przez przechowywanie tokenu uwierzytelniającego (np. JWT) lub ciasteczka sesyjnego.

Użytkownik musi mieć możliwość wylogowania się w każdej chwili. Przycisk „Wyloguj” powinien być łatwo dostępny z interfejsu użytkownika i skutecznie kończyć sesję, aby zabezpieczyć dane użytkownika — szczególnie przy korzystaniu z aplikacji na współdzielonym urządzeniu.

Kryteria akceptacji (Acceptance Criteria)

- Użytkownik może utworzyć konto z poprawnym adresem e-mail i hasłem.
- Po rejestracji użytkownik zostaje zalogowany lub przekierowany na ekran logowania.
- Próba logowania z nieprawidłowymi danymi kończy się odpowiednim komunikatem o błędzie.
- Po zalogowaniu użytkownik widzi ekran główny aplikacji z dostępem do funkcji.
- Kliknięcie przycisku „Wyloguj” kończy sesję użytkownika i przekierowuje na ekran logowania.
- Dane uwierzytelniające są przechowywane w bezpieczny sposób (np. hasła są hashowane).

Uwagi dla architekta / testera / dewelopera

- System powinien korzystać z bezpiecznego mechanizmu autoryzacji – np. JWT lub sesje HTTP-only cookies.
- Hasła powinny być przechowywane w bazie danych jako zahashowane wartości (np. bcrypt, Argon2).
- Należy dodać walidację danych wejściowych — np. e-mail w odpowiednim formacie, mocne hasło.
- Formularze rejestracji i logowania muszą być odporne na ataki CSRF i XSS.
- Testerzy powinni zweryfikować:
  - poprawność komunikatów błędów,
  - skuteczność wylogowywania,
  - brak możliwości dostępu do danych po wylogowaniu (nawet przez przycisk „Wstecz” w przeglądarce),
  - logikę błędnych danych przy rejestracji/logowaniu (np. już istniejący e-mail).

Diagram przypadków użycia (Use Cases)