# Wymagania bezpieczeństwa:

1. Bezpieczne logowanie: Umożliwienie bezpiecznego logowania i zarządzania kontami użytkowników, przy pomocy unikatowego loginu oraz hasła, autoryzacja e-mail, oraz procedury resetowania hasła.
2. Ochrona danych użytkowników: Zabezpieczenie danych logowania i informacji osobistych użytkowników za pomocą szyfrowania.
3. Szyfrowane połączenie: Używanie protokołu HTTPS do zabezpieczenia transmisji danych między przeglądarką a serwerem.
4. Regularne aktualizacje: Stałe aktualizacje oprogramowania w celu łatania luk bezpieczeństwa i zapobiegania atakom.
5. Ochrona przed atakami sieciowymi: Wykorzystanie narzędzi do wykrywania i neutralizacji ataków DDoS.
6. Bezpieczeństwo treści: Skanowanie i weryfikacja treści przesyłanych przez użytkowników.
7. Monitorowanie i reakcja na incydenty: System monitorowania aktywności w celu szybkiego wykrywania i reagowania na potencjalne zagrożenia.
8. Szkolenie w zakresie bezpieczeństwa: Edukacja użytkowników odnośnie bezpiecznego korzystania z aplikacji.