# Polityka bezpieczeństwa projektu aplikacji z programowania zespołowego

## Opis problemu

Zaimplementowanie systemu opartego na połączeniu wielu urządzeń mobilnych z serwerem obsługującym proces inwentaryzacji zapewniającego względne bezpeczeństwo danych. Produkt skierowany jest do instytucji oferujących dobra majątkowe oraz posiadających spis oferowanych produktów w formie elektronicznej (np. bazy danych). Sercem aplikacji będzie serwer pozwalający na zarządzanie procesem inwentaryzacji, którą przeprowadzać będą pracownicy wyposażeni w smartfony z dostępem do sieci oraz zainstalowaną aplikacją udostępnianą przez dewelopera. Do połączenia serwera oraz klientów w postaci smartfonów wykorzystywana jest technologia Wi-Fi (sieć lokalna), której zasięg działania oraz względy bezpieczeństwa stoją na poziomie wystarczającym do zrealizowania postawionych celów. Wszystkie wprowadzane dane, zarówno przez inwentaryzującego jak i nadzorującego, przechowywane będą w bazie danych, które aktualnie są standardem do tego typu zastosowań. Dzięki zastosowaniu tej technologii wszystkie dane będą bezpieczne, łatwo dostępne dla użytkownika oraz pozwolą na wprowadzanie dodatkowych funkcji, takich jak generowanie raportu podsumowującego przebieg inwentaryzacji.

## Elementy wymagające zabezpieczenia

1. dostęp do bazy danych,
2. sposób przechowywania haseł w bazie danych,
3. przesył danych pomiędzy aplikacją kliencką i serwerową,
4. dostęp do aplikacji serwerowej oraz klienckiej,
5. dostęp do poszczególnych opcji dla danych użytkowników (pracownik, nie ma prawa do tworzenia kont, czy też zmieniania uprawnień),
6. sposób ustanowienia połączenia.

## Sposób zabezpieczenia

Ad 1. dostęp do bazy danych jest możliwy jedynie lokalnie, a także wymagane jest hasło uwierzytelniające dla danego użytkownika. Hasło jest złożone z przynajmniej 15 znaków w tym co najmniej 3 cyfry, 2 znaki specjalne, co najmniej jedna duża i jedna mała litera,

Ad 2. hasła użytkowników przechowywane są w bazie danych pod postacią hashy, funkcją hashującą jest algorytm `bcrypt`, algorytm ten generuje automatycznie sól odpowiedniej długości,

Ad 3. przesył danych pomiędzy aplikacją kliencką i serwerową odbywa się w obrębie zabezpieczonej sieci `Wi-Fi`, co za tym idzie tylko podłączeni użytkownicy mogą przechwycić wiadomość. Dodatkowo w routerze można ustawić filtrowanie adresów MAC, poprawiając tym samym stopień bezpieczeństwa, gdyż wtedy potencjalny atakujący musiałby posiadać klucz do sieci, a także być wpisany na `whitelist` adresów MAC. Dodatkowo wiadomości szyfrowane są kluczem uzyskanym podczas skanowania kodu QR, przy próbie połączenia. Jest to szyfrowanie symetryczne,

Ad 4. dostęp do aplikacji zarówno ze strony klienckiej jak i serwerowej, chroniony jest hasłem, przechowywanym w bazie danych pod postacią hashy (`Ad 2.`), po 3 próbach, konto użytkonika zostaje zablokowane i może zostać odblokowane jedynie poprzez kontak z serwisem,

Ad 5. każde z kont użytkowników ma ograniczony dostęp do funkcjonalności programu. Dla przykładu jedynie konto z uprawnieniami administratora może zarządzać kontami innych użytkowników.

Ad 6. połączenie pomiędzy aplikacją kliencką a serwerową odbywa się poprzez skanowanie kodu QR, wyświetlanego w aplikacji serwerowej, przez aplikację kliencką. Podczas tego procesu aplikacja kliencka, dostaje informację o adresie IP aplikacji serwerowej w sieci, a także klucz prywatny potrzebny do szyfrowania wiadomości przesyłanych do aplikacji serwerowej.