Zgodność reprezentacji

Zgodność pomiędzy specyfikacją funkcjonalną, a projektem wysokiego poziomu i projektem niskiego poziomu

1. Audytowanie

Funkcjonalne wymagania bezpieczeństwa	**Opis funkcji bezpieczeństwa**	**Interfejs - wysoki poziom**	**Interfejs - niski poziom**	**Uzasadnienie**
FAU_ARP FAU_ARP.1 FAU_ARP.1.1 FAU_ARP.1.2	Dane audytowe przechowywane w bazie danych	Wszystkie metody interfejsu	Wszystkie metody interfejsu	Każda akcja systemu wykonywana przez użytkownika przechowywana jest w bazie danych
FAU_GEN FAU_GEN.1 FAU_GEN.2 FAU_GEN.2.1	Przechowywanie danych o działaniach potencjalnie niebezpiecznych dla systemu	Komponent: Policies	Klasy: UserManager, LogsManager, AuthManager	Podczas uwierzytelniania może dojść do naruszenia bezpieczeństwa danych. Szczególna uwaga zwrócona na nieprawidłowości występujące podczas logowania
FAU_SAR FAU_SAR.1 FAU_SAR.1.1 FAU_SAR.1.2 FAU_SAR.2 FAU_SAR.2.1	Ograniczenie dostępu do danych audytowych	Brak metod	Brak metod	Brak innej możliwości dostania się do danych audytowych. Dostęp do danych jedynie przez bezpośrednie zalogowanie użytkownika. Brak wystawionych metod umożliwiających dostęp do danych audytowych
FAU_STG FAU_STG.1 FAU_STG.1.1 FAU_STG.2 FAU_STG.2.1	Tworzenie kopii zapasowej z użyciem specjalistycznego narzędzia	Brak metod	Brak metod	Kopie zapasowe tworzone cyklicznie za pomocą narzędzia do zarządzania bazami danych

2. Weryfikacja

Funkcjonalne wymagania bezpieczeństwa	**Opis funkcji bezpieczeństwa**	**Interfejs - wysoki poziom**	**Interfejs - niski poziom**	**Uzasadnienie**

Funkcjonalne wymagania bezpieczeństwa	Opis funkcji bezpieczeństwa	Interfejs - wysoki poziom	Interfejs - niski poziom	Uzasadnienie
FDP_ACC FDP_ACC.1	Działanie wg polityki kontroli dostępu	Komponenty: Policies, RequestValidator, UserManagement	Klasy: AuthManager, PermissionManager Metody: putUser, postUser, logoutUser, deletePerm, getPerm, getPermID	System pobiera rolę użytkowników i na ich podstawie zezwala na wykonanie pewnych operacji
FDP_ACF.1 FDP_ACF.1.1	Funkcje systemu dostępne tylko dla ograniczonego grona użytkowników	Komponenty: Policies, UserManagment	Klasa: PermissionManager, Metody: deletePerm, getPerm, getPermID	System pobiera rolę, do których należy użytkownik i na ich podstawie umożliwia dostęp do informacji
FDP_ACF.1.1 FDP_ACF.1.2	Dane w bazie danych mają swoich autorów i czas utworzenia	Brak metod	Brak metod	Każde dane tworzone w systemie posiadają swojego autora i ostatnie zmiany i czas utworzenia

3. Uwierzytelnianie

Funkcjonalne wymagania bezpieczeństwa	Opis funkcji bezpieczeństwa	Interfejs - wysoki poziom	Interfejs - niski poziom	Uzasadnienie
FIA_AFL FIA_AFL.1.1 FIA_AFL.1.2	Reagowanie na błędy uwierzytelniania	Komponent: RequestValidator, UserManagement	Klasy: AuthManager, LogsManager, metody: getLogs, postUser	Nieudane wielokrotne próby logowania na jedno z kont prowadzi do wprowadzania blokady - możliwość logowania na to konto zostanie wstrzymana
FDP_ACF.1 FIA_UAU.1 FIA_UAU.1.1 FIA_UAU.1.2	Sprawdzenie czy użytkownik jest zalogowany przed wykonaniem operacji	Komponent: UserManagement	Klasy: UserManager, LogsManager, PermissionManager metody: getLogs, getPerms, getUser	Pobieranie informacji czy użytkownik jest zalogowany na podstawie sesji

Funkcjonalne wymagania bezpieczeństwa	Opis funkcji bezpieczeństwa	Interfejs - wysoki poziom	Interfejs - niski poziom	Uzasadnienie
FIA_UID FIA_UID.1 FIA_UID.1.1	Identyfikacja użytkownika, mechanizm uwierzytelniania	Komponenty: UserManagement, Policies	Klasy: AuthManager, UserManager, LogsManager Metody: putUser, postUser, logoutUser, getUserId	Po zalogowaniu każdy użytkownik otrzymuje swój token, informacja ta jest przechowywana w sesji - daje nam to możliwość sprawdzenia użytkownika

4. Przerwanie procesu

Funkcjonalne wymagania bezpieczeństwa	Opis funkcji bezpieczeństwa	Interfejs - wysoki poziom	Interfejs - niski poziom	Uzasadnienie
FDP_IFF FDP_IFF.1 FDP_IFF.1.1	Kontrola przepływu informacji między węzłami komunikacyjnymi	Wszystkie metody interfejsu	Wszystkie metody interfejsu	Działania systemu oparte są na bezpiecznym kanale SSL.

5. Ochrona

Funkcjonalne wymagania bezpieczeństwa	Opis funkcji bezpieczeństwa	Interfejs - wysoki poziom	Interfejs - niski poziom	Uzasadnienie
FMT_SMR FMT_SMR.1 FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMR.2 FMT_SMR.2.1 FMT_SMR.2.2	Prawa przyznawane na podstawie zdefiniowanych ról	Komponenty: UserManagement, DocumentManagement	Klasy: ShareManager, PermissionManager, UserManager. Metody: getUser, getPerm, getShare, getPermID	Przyznane funkcje dla użytkownika można sprawdzić na podstawie przypisanych do niego ról

Funkcjonalne wymagania bezpieczeństwa	Opis funkcji bezpieczeństwa	Interfejs - wysoki poziom	Interfejs - niski poziom	Uzasadnienie
FPT_STM FPT_STM.1 FPT_STM.1.1	Stosowanie znaczników czasu	Wszystkie metody interfejsu	Wszystkie metody interfejsu	Wszystkim danym przechowywanym w bazie danych przyznawany jest rekord - czas dokonania / czas dokonania zmian, który pobierany jest z systemu. Następnie synchronizuje się z własnym serwerem czasu.