项目文档

# Functional Requirement

ID Function Requirement  
DATA-VALIDATION-001 Data Validation The system shall validate all user-entered data in real-time to ensure correctness and consistency.  
DATA-VALIDATION-002 Data Validation The system shall display or hide data entry fields dynamically based on the selected case or incident type.  
DATA-ENTRY-001 Data Entry The system shall allow users to enter data in an offline mode, storing the data locally until synchronization.  
DATA-ENTRY-002 Data Entry The system shall provide a mechanism for users to flag entries as "high priority," ensuring immediate synchronization when connectivity is restored.  
DATA-ENTRY-003 Data Entry The system shall support voice input for data entry and search, with accuracy and ease of use for field officers.  
CONFLICT-RESOLUTION-001 Conflict Resolution The system shall detect conflicts when the same record is modified in both field and office environments and allow users to manually resolve these conflicts, preserving both versions.  
UI-ACCESS-001 User Interface The system shall provide role-specific dashboards and menus to tailor the user interface to the responsibilities and workflows of each role.  
SEARCH-001 Search Functionality The system shall support natural language search for case and suspect data, allowing users to input queries in plain language.  
SEARCH-002 Search Functionality The system shall allow users to filter search results by the following criteria: date range, assigned officer, case status, location tags, and incident type.  
SEARCH-003 Search Functionality The system shall allow users to perform record lookup and data entry in offline environments.  
SECURITY-001 Security The system shall implement granular, role-based access control to ensure that users can only access specific data types as permitted by their role.  
SECURITY-002 Security The system shall record all changes to case and suspect records, including the user who made the change, timestamp, old and new values, and optional comments.  
SECURITY-003 Security The system shall allow users to view historical versions of records to identify and resolve discrepancies.

# External Description

# 5 Constraints  
  
## 5.1 Regulatory/Legal Constraints  
  
The system shall pass a third-party audit by a certified ISO/IEC 27001 auditor with no critical findings. The system shall comply with all relevant data protection laws, including the General Data Protection Regulation (GDPR) and the Personal Data Protection Bill (PDPB).  
  
## 5.2 Hardware Constraints  
  
The system shall operate on Android and iOS devices with a minimum of 2GB RAM and 10GB storage. The system shall not require any specialized hardware beyond standard mobile devices.  
  
## 5.3 Interface Constraints  
  
The system shall provide a user interface for data entry and search. The system shall support voice input with an accuracy rate of at least 95%, as measured by a standardized speech recognition test involving 1000 audio samples.  
  
## 5.4 Design and Implementation Constraints  
  
The system shall use a RESTful API for data synchronization. The system shall flag invalid entries for correction using a pop-up notification and shall provide a clear description of the validation error.  
  
## 5.5 Other Constraints  
  
The system shall restrict read-only access to restricted data for users with the role of "Analyst". The system shall synchronize a 500MB dataset within 10 minutes on a 2G network with a success rate of at least 95%.