# Functional Requirement

✅ Functional Requirements for CCTNS System  
FR 1: Complaint Registration  
Input: Incident details (date, time, location, type of crime), citizen information (name, contact)  
Output: Generated FIR number, confirmation message via SMS/email  
Description: The system allows citizens to register complaints online. Input data is validated, and a unique FIR is generated.  
FR 2: FIR Tracking  
Input: FIR number or citizen ID  
Output: Current status of the FIR, case details, and history  
Description: Users can track the progress of their complaint or FIR using an assigned FIR number or personal identification.  
FR 3: Case Management  
Input: FIR details, investigation notes, evidence files, officer assignments  
Output: Updated case file with timestamps and alerts for pending actions  
Description: Officers can update case status, add notes, upload evidence, and assign tasks to other officers.  
FR 4: Court Interaction  
Input: Court orders, hearing dates, legal documents  
Output: Updated court timeline, reminders for upcoming hearings  
Description: Legal officers can manage court proceedings, submit documents, and receive notifications about scheduled hearings.  
FR 5: Criminal Profile Management  
Input: Personal and biometric data of individuals (e.g., name, age, fingerprints)  
Output: Criminal profile and history report  
Description: Maintains and updates profiles of known criminals based on past convictions and current activities.  
FR 6: Advanced Search and Reporting  
Input: Filters such as name, location, date, crime type  
Output: List of matching cases or persons, reports in PDF/Excel format  
Description: Allows authorized users to search for specific data and generate detailed reports.  
FR 7: Role-Based Access Control  
Input: User login credentials  
Output: Access to features based on user role  
Description: Ensures that only authorized users can access certain modules and functions according to their roles.  
FR 8: Configuration and Customization  
Input: Admin preferences for layout, workflows, and notification settings  
Output: Modified system behavior to meet local policing needs  
Description: Administrators can customize the system interface and workflow to suit regional or departmental requirements.  
FR 9: Case Type Management  
Input: Case type name, description, applicable legal statutes  
Output: Updated case type list  
Description: System allows administrators to add, modify, or delete case types used by police when creating new cases.  
FR 10: Suspect Management  
Input: Suspect's name, gender, age, contact info, initial charges  
Output: Suspect record ID and associated case information  
Description: Supports temporary suspect registration and links suspects to relevant cases for further investigation.  
FR 11: Evidence Management  
Input: Evidence name, type (physical, video, audio), upload time, uploaded by  
Output: Evidence archive ID, download link  
Description: Provides secure upload and storage of digital evidence, with support for retrieval by case or time.  
FR 12: Automated Notification System  
Input: Case status change event (e.g., “Evidence Collected”, “Arrest Made”)  
Output: SMS or email notification sent to designated users  
Description: Sends automated alerts to relevant stakeholders upon key case events or due dates.  
FR 13: Data Analysis and Statistical Reporting  
Input: Time range, region, case type filters  
Output: Graphical and tabular reports (PDF/Excel) showing crime trends  
Description: Generates statistical reports and visualizations for crime analysis and policy planning.  
FR 14: Multilingual Support  
Input: User language preference setting  
Output: UI displayed in selected language  
Description: The system supports multiple languages (e.g., Hindi, English, Tamil) to accommodate diverse user bases.  
FR 15: Mobile Application Functionality  
Input: Camera input, voice recording, GPS location, offline form entry  
Output: Field data stored locally and synchronized when online  
Description: Mobile app supports offline case drafting, photo/video capture, and automatic sync once connectivity is restored.

# External Description

3. External Interfaces  
3.1 User Interfaces  
Web-based dashboard for police and legal officials  
Mobile-friendly citizen portal  
Desktop application for backend administrative tasks  
3.2 Hardware Interfaces  
CCTV integration via IP cameras  
Biometric scanners for identity verification  
Printers for generating reports and FIRs  
3.3 Software Interfaces  
Integration with e-Courts project for case tracking  
Linkage with Aadhaar database for citizen verification  
Email/SMS gateway for notifications  
3.4 Communication Interfaces  
Secure HTTPS communication between client and server  
Encrypted data transfer using TLS 1.2 or higher  
Inter-system messaging through RESTful APIs