# Functional Requirement

3.1 Complaint Registration

Input: Complainant information, incident description, time & location, evidence (images/documents)

Output: Complaint ID, confirmation notice, status-tracking link

Description: Citizens can file formal complaints via web or mobile app. The system auto-generates a unique ID and sends a confirmation by SMS/email.

3.2 Investigation Tracking

Input: Case ID, investigation progress, suspect details, evidence log

Output: Updated case status, record of uploaded attachments

Description: Investigators can update case progress, including suspect identification, interrogation notes, and evidence uploads.

3.3 Court Case Management

Input: Case ID, hearing date, judge’s comments, verdict

Output: Updated court records, status-change notification

Description: Judges or clerks enter court proceedings into the system for police review and follow-up.

3.4 Advanced Search & Analytics

Input: Name, ID number, case type, date range, geographic location

Output: Filtered case list, visual charts (e.g., crime-trend graphs)

Description: Multi-dimensional keyword/attribute queries with statistical tools to aid decision-making.

3.5 Role-Based Access Control

Input: User credentials, permission-group configuration

Output: Personalized interface, permission-limit alerts

Description: Different roles (citizen, officer, judge) have distinct permissions and UIs to ensure data security.

3.6 Security & Authentication

Input: Username, password, biometrics (fingerprint/face), CAPTCHA

Output: Login success message, session token, audit log

Description: Multi-factor authentication with all sensitive actions logged to prevent unauthorized access.

3.7 Citizen Portal

Input: Complaint ID, user account info

Output: Progress updates, notifications, feedback channel

Description: Online status checking, SMS/email alerts, and satisfaction surveys to boost public engagement.

3.8 Criminal Record Management

Input: Suspect name, ID number, prior convictions, photo

Output: Create/update criminal profile, history display

Description: Maintains searchable suspect records for quick retrieval and comparison.

3.9 Evidence Management

Input: Evidence ID, source, storage location, custodian

Output: Digital evidence archive, borrowing log, destruction workflow

Description: Centralized management of physical and digital evidence ensuring integrity and traceability.

3.10 Incident Reporting

Input: Location, time, involved persons, preliminary assessment

Output: Report record, supervisory approval status

Description: Officers can quickly log incidents on-scene; the system routes them for departmental approval.

3.11 Mobile Integration

Input: Device GPS, voice input, camera

Output: Mobile case entry, real-time sync, offline cache

Description: Officers use phones/tablets for on-site investigations; data syncs live or saves offline.

3.12 Notification System

Input: Status change, approval completion, overdue alert

Output: SMS, email, push notification

Description: Automatic alerts to relevant parties per rules, ensuring timely task handling.

3.13 Multi-Language Support

Input: User-selected language preference

Output: Interface rendered in chosen language

Description: Supports Chinese, English, and regional dialects for multi-ethnic areas.

3.14 Data Export & Reporting

Input: Query criteria, export format (PDF/Excel)

Output: Data report file

Description: Exports case data in standard formats for analysis and higher-level reporting.

3.15 Audit Trail

Input: User actions (add, modify, delete)

Output: Audit-log entries

Description: Logs all critical actions—timestamp, user ID, IP—for accountability.

3.16 Integration with External Systems

Input: External API requests (e.g., police database, judicial platform)

Output: Data exchange, API response

Description: Standardized interfaces share data with other government systems (traffic violations, prison management, etc.).