# Functional Requirement

1.1 Complaint Registration Function   
 Function ID: FR-01   
 Description: Citizens can submit complaints through the system. The system will generate a unique complaint ID and assign the complaint to an appropriate police personnel for investigation.   
 Input: Nature of the complaint, date and time of the incident, location, detailed description, and optional supporting documents.   
 Output: A registered complaint with a unique complaint ID, a confirmation message sent to the citizen, and a notification to the assigned police personnel.   
  
1.2 Manage Investigation Function   
 Function ID: FR-02   
 Description: Police personnel can update the investigation status, add notes, and attach new evidence to an investigation case.   
 Input: Investigation case ID, new status, notes, and optional supporting documents.   
 Output: Updated investigation case with new status and notes, notification to the citizen and relevant court case handler, and a logged modification for audit purposes.   
  
1.3 View Investigation Details Function   
 Function ID: FR-03   
 Description: Police personnel can view the details of an investigation case, including associated complaints, current status, assigned personnel, and evidence.   
 Input: Investigation case ID and optional search or filtering criteria.   
 Output: Displayed investigation details, and if sensitive data is accessed, a logged activity for audit purposes.   
  
1.4 Update Investigation Status Function   
 Function ID: FR-04   
 Description: Police personnel can update the status of an investigation case and optionally add notes or supporting documents.   
 Input: Investigation case ID, new status, and optional notes or documents.   
 Output: Updated investigation status in the system, linked to the associated complaint and court case, and notifications sent to the citizen and court case handler.   
  
1.5 Add Criminal Record Function   
 Function ID: FR-05   
 Description: Police personnel can add a new criminal record to the system, which is linked to an investigation or court case.   
 Input: Criminal information (name, age, offense description), evidence, and associated investigation or court case ID.   
 Output: A new criminal record with a unique record ID, linked to the selected case, and a confirmation message sent to the police personnel.   
  
1.6 Modify Criminal Information Function   
 Function ID: FR-06   
 Description: Police personnel can modify an existing criminal record in the system, including criminal details, offense description, or evidence.   
 Input: Criminal record ID, updated criminal information, and optional notes or documents.   
 Output: Updated criminal record, linked to the associated investigation or court case, a confirmation message, and a logged modification for audit purposes.   
  
1.7 Delete Criminal Record Function   
 Function ID: FR-07   
 Description: Police personnel can delete a criminal record from the system.   
 Input: Criminal record ID and confirmation for deletion.   
 Output: Deleted criminal record, updated associated investigation or court case, a confirmation message, and a logged deletion for audit purposes.   
  
1.8 View Court Case Details Function   
 Function ID: FR-08   
 Description: Police personnel or citizens can view the details of a court case, including status, associated complaint or investigation, and scheduled court dates.   
 Input: Court case ID and optional search or filtering criteria.   
 Output: Displayed court case details, and if sensitive data is accessed, a logged activity for audit purposes.   
  
1.9 Update Court Case Status Function   
 Function ID: FR-09   
 Description: Police personnel can update the status of a court case and optionally add comments or supporting documents.   
 Input: Court case ID, new status, and optional comments or documents.   
 Output: Updated court case status, linked to the associated complaint or investigation, a notification to the citizen, and a logged modification for audit purposes.   
  
1.10 Manage Court Interaction Function   
 Function ID: FR-10   
 Description: Police personnel or administrators can update court case information, such as court decisions, timelines, or legal documents.   
 Input: Court case ID, updated court case details, and optional supporting documents.   
 Output: Updated court case, linked to the associated complaint or investigation, notifications to relevant stakeholders, and a logged modification for audit purposes.   
  
1.11 View Citizen Information Function   
 Function ID: FR-11   
 Description: Police personnel can view the personal and case-related information of a citizen.   
 Input: Citizen ID and optional search or filtering criteria.   
 Output: Displayed citizen information, and if sensitive data is accessed, a logged activity for audit purposes.   
  
1.12 Update Citizen Profile Function   
 Function ID: FR-12   
 Description: Administrators or police personnel can update the personal or contact information of a citizen.   
 Input: Citizen ID and updated information (e.g., contact details, address).   
 Output: Updated citizen profile in the system, a confirmation message, and a logged modification for audit purposes.   
  
1.13 Register Police Personnel Function   
 Function ID: FR-13   
 Description: Administrators can register new police personnel in the system, assigning them a unique personnel ID and login credentials.   
 Input: Police personnel information (name, role, department, contact information, and authentication details).   
 Output: Registered police personnel with a unique ID, confirmation message, and a logged registration for audit purposes.   
  
1.14 Assign Role to User Function   
 Function ID: FR-14   
 Description: Administrators can assign a predefined role to a user (citizen or police personnel), which determines their access rights and responsibilities.   
 Input: User ID and selected role.   
 Output: Updated user profile with the new role, updated access control policies, and a logged assignment for audit purposes.   
  
1.15 Modify Role Permissions Function   
 Function ID: FR-15   
 Description: Administrators can modify the permissions associated with a user role, such as enabling or disabling specific access rights.   
 Input: Role name or ID and updated permissions.   
 Output: Updated role permissions, updated access control policies, a confirmation message, and a logged modification for audit purposes.   
  
1.16 Configure System Settings Function   
 Function ID: FR-16   
 Description: Administrators can configure system-wide settings, such as security policies, notification preferences, or access control rules.   
 Input: Configuration category and new settings (e.g., system timeout, password policy).   
 Output: Updated system settings, confirmation message, and a logged configuration change for audit purposes.   
  
1.17 Update Configuration Function   
 Function ID: FR-17   
 Description: Administrators can update existing system configurations, such as access control rules or notification settings.   
 Input: Configuration ID and updated values.   
 Output: Updated configuration settings, confirmation message, and a logged modification for audit purposes.   
  
1.18 Manage Security Features Function   
 Function ID: FR-18   
 Description: Administrators can enable, disable, or modify security features, such as two-factor authentication or encryption settings.   
 Input: Security feature name or ID and new status or settings.   
 Output: Updated security feature configuration, confirmation message, and a logged modification for audit purposes.   
  
1.19 Ensure Data Integrity Function   
 Function ID: FR-19   
 Description: The system performs data integrity checks to verify the consistency of stored data (e.g., complaints linked to investigations or user roles aligned with access rights).   
 Input: System data entities (e.g., complaint, criminal record, court case).   
 Output: Data integrity report with flagged inconsistencies, confirmation message, and a logged integrity check for audit purposes.   
  
1.20 Control Access Rights Function   
 Function ID: FR-20   
 Description: Administrators can modify the access rights of a user (citizen or police personnel) to specific system functions.   
 Input: User ID and updated access rights (e.g., "View Court Case", "Modify Complaint").   
 Output: Updated user access rights, confirmation message, and a logged modification for audit purposes.   
  
1.21 View Access Logs Function   
 Function ID: FR-21   
 Description: Administrators or authorized police personnel can view access logs, which include information about user activity and data access.   
 Input: Search criteria such as user ID, date range, or activity type.   
 Output: Displayed access logs, and the viewing activity is logged for audit purposes.   
  
1.22 Track Case Progress Function   
 Function ID: FR-22   
 Description: Police personnel or citizens can track the progress of an investigation or court case, including status updates and timelines.   
 Input: Case ID (investigation or court case) and optional filtering criteria.   
 Output: Displayed case progress, and if sensitive data is accessed, the activity is logged for audit purposes.   
  
1.23 Manage Case Complaint Link Function   
 Function ID: FR-23   
 Description: Police personnel or administrators can create, modify, or remove the link between a case and a complaint.   
 Input: Case ID (investigation or court case) and complaint ID.   
 Output: Updated case-complaint relationship, confirmation message, and a logged modification for audit purposes.   
  
1.24 View Police Personnel Function   
 Function ID: FR-24   
 Description: Administrators or authorized personnel can view the personal and professional details of a police officer.   
 Input: Police personnel ID and optional search or filtering criteria.   
 Output: Displayed police personnel information, and if sensitive data is accessed, the activity is logged for audit purposes.   
  
1.25 View Data Integrity Function   
 Function ID: FR-25   
 Description: Administrators can view the system’s data integrity status, including reports on inconsistencies or errors.   
 Input: Filtering criteria such as data entity type (e.g., complaint, criminal record) and time range.   
 Output: Displayed data integrity report, and the viewing activity is logged for audit purposes.   
  
1.26 View Access Control Function   
 Function ID: FR-26   
 Description: Administrators can view the current access control policies and user permissions.   
 Input: Filtering criteria such as role name or permission type.   
 Output: Displayed access control policies, and the viewing activity is logged for audit purposes.   
  
1.27 Manage Court Case Function   
 Function ID: FR-27   
 Description: Administrators or police personnel can update court case details, such as status, legal documents, or case timelines.   
 Input: Court case ID and updated case information.   
 Output: Updated court case in the database, notifications to relevant stakeholders, and a logged modification for audit purposes.   
  
1.28 Manage Citizen Function   
 Function ID: FR-28   
 Description: Administrators or police personnel can modify a citizen’s profile, including personal and contact information.   
 Input: Citizen ID and updated information.   
 Output: Updated citizen profile in the database, a confirmation message, and a logged modification for audit purposes.