项目文档

# Functional Requirement

1. Functional Requirements  
  
1.1 Complaint Registration Function   
Function ID: FR-01   
Description: Citizens can register a new complaint with detailed incident information and supporting documents.   
Input: Incident description, location, date, supporting documents, citizen ID.   
Output: A unique complaint ID, confirmation message, and complaint data stored in the database.  
  
1.2 View Complaint Details Function   
Function ID: FR-02   
Description: Police Personnel and Administrators can view detailed information about a complaint, including its current status and any related automated investigation data.   
Input: Valid complaint ID and user login credentials.   
Output: Complaint details, including incident description, location, date, status, and associated automated investigation information.  
  
1.3 Update Complaint Status Function   
Function ID: FR-03   
Description: Police Personnel and Administrators can update the status of a complaint and provide an optional comment.   
Input: Valid complaint ID, new status, optional comment.   
Output: Updated complaint status in the database, status change logged in the ComplaintStatusLog, and a notification sent to the Citizen.  
  
1.4 Delete Complaint Record Function   
Function ID: FR-04   
Description: Administrators can permanently delete a complaint record from the system.   
Input: Valid complaint ID and confirmation from the Administrator.   
Output: Deleted complaint record, deletion logged in the system, and notification sent to the Citizen and associated Police Personnel.  
  
1.5 Automated Investigation Initiation Function   
Function ID: FR-05   
Description: Police Personnel and Administrators can initiate an automated investigation for a registered complaint.   
Input: Valid complaint ID and user login credentials.   
Output: AutomatedInvestigation record created in the database, complaint status updated to "Automated Investigation In Progress," and notification sent to relevant Police Personnel.  
  
1.6 Modify Investigation Data Function   
Function ID: FR-06   
Description: Police Personnel and Administrators can modify data associated with an ongoing automated investigation, such as evidence, witness information, or investigation notes.   
Input: Valid complaint ID, editable investigation fields (e.g., evidence, notes), and user login credentials.   
Output: Updated AutomatedInvestigation data, complaint status updated if necessary, and notification sent to the Citizen and associated Police Personnel.  
  
1.7 View Investigation Progress Function   
Function ID: FR-07   
Description: Citizens, Police Personnel, and Administrators can view the progress of an automated investigation.   
Input: Valid complaint ID and user login credentials.   
Output: InvestigationProgress details displayed, access logged in the system, and any additional information such as pending actions or findings.  
  
1.8 Court Case Registration Function   
Function ID: FR-08   
Description: Administrators and Police Personnel can register a new court case linked to a complaint.   
Input: Valid complaint ID, court name, case type, filing date, and involved parties.   
Output: CourtCase record created and stored in the database, linked to the complaint, and notification sent to the Citizen.  
  
1.9 Update Court Case Status Function   
Function ID: FR-09   
Description: Police Personnel and Administrators can update the status of a court case and provide an optional comment.   
Input: Valid court case ID, new status, optional comment.   
Output: Updated court case status in the database, status change logged in the CaseStatusLog, and notification sent to the Citizen.  
  
1.10 View Court Case Details Function   
Function ID: FR-10   
Description: Citizens, Police Personnel, and Administrators can view detailed information about a court case, including related complaint data.   
Input: Valid court case ID and user login credentials.   
Output: CourtCase details displayed, access logged in the system, and related complaint information if applicable.  
  
1.11 Delete Court Case Record Function   
Function ID: FR-11   
Description: Administrators can permanently delete a court case record from the system.   
Input: Valid court case ID and confirmation from the Administrator.   
Output: Deleted court case record, deletion logged in the system, and notification sent to the Citizen and associated Police Personnel.  
  
1.12 Search for Crimes Function   
Function ID: FR-12   
Description: Police Personnel and Administrators can search for crime-related data using criteria such as keyword, date range, or location.   
Input: Search criteria (e.g., keyword, date, location).   
Output: List of matching crime-related records (complaints or court cases) with summary information and a log of the search activity.  
  
1.13 Search for Criminals Function   
Function ID: FR-13   
Description: Police Personnel and Administrators can search for criminal records using criteria such as name, age range, gender, or case ID.   
Input: Search criteria (e.g., name, age range, gender, case ID).   
Output: List of matching criminal records with summary information and a log of the search activity.  
  
1.14 Search for Investigation Records Function   
Function ID: FR-14   
Description: Police Personnel and Administrators can search for investigation records using complaint ID, investigation status, or keywords.   
Input: Search criteria (e.g., complaint ID, status, keyword).   
Output: List of matching investigation records with summary details and a log of the search activity.  
  
1.15 Citizen Submit Complaint Function   
Function ID: FR-15   
Description: Citizens can submit a new complaint through the system by filling out a form and uploading supporting documents.   
Input: Incident description, location, date, supporting documents, and valid citizen ID.   
Output: A unique complaint ID generated, complaint data stored in the database, and confirmation message sent to the Citizen.  
  
1.16 Citizen View Complaint Status Function   
Function ID: FR-16   
Description: Citizens can view the current status of a previously submitted complaint.   
Input: Valid complaint ID and user login credentials.   
Output: Complaint status displayed, including the stage of the automated investigation and any recent updates.  
  
1.17 Police Personnel Manage Complaints Function   
Function ID: FR-17   
Description: Police Personnel and Administrators can manage complaints by updating their status, escalating them, or adding notes.   
Input: Valid complaint ID and management action (e.g., update, escalate, add notes).   
Output: Updated complaint data in the database, management action logged, and notification sent to the Citizen if configured.  
  
1.18 Police Personnel Manage Investigations Function   
Function ID: FR-18   
Description: Police Personnel and Administrators can manage automated investigations by updating findings, pausing the investigation, or escalating to manual review.   
Input: Valid complaint ID and management action (e.g., update findings, pause, escalate).   
Output: Updated AutomatedInvestigation data, complaint status updated, and notification sent to the Citizen if configured.  
  
1.19 Administrator Manage Users Function   
Function ID: FR-19   
Description: Administrators can manage user accounts (Citizens, Police Personnel, and other Administrators) by creating, updating, or deleting them.   
Input: User details (e.g., name, role, contact information) and action (e.g., create, update, delete).   
Output: Updated user records in the database, management action logged, and notification sent to the affected user if configured.  
  
1.20 Administrator Configure System Settings Function   
Function ID: FR-20   
Description: Administrators can configure system-wide settings such as notification preferences, access control rules, and automated investigation parameters.   
Input: System settings configuration (e.g., notification settings, access rules).   
Output: Updated system settings stored in the database, configuration action logged, and new settings applied to the system.  
  
1.21 Manage Investigation Progress Function   
Function ID: FR-21   
Description: Police Personnel and Administrators can update the progress of an automated investigation, such as adding notes or marking a stage as completed.   
Input: Valid complaint ID and progress details (e.g., stage completed, findings).   
Output: Updated InvestigationProgress data, complaint status adjusted, and notification sent to the Citizen if configured.  
  
1.22 Manage Case Status Log Function   
Function ID: FR-22   
Description: Administrators and Police Personnel can view, edit, or delete entries in the CaseStatusLog to track changes in court case statuses.   
Input: Valid court case ID and action (e.g., view, edit, delete).   
Output: Updated CaseStatusLog data, management action logged, and notification sent to relevant personnel if configured.  
  
1.23 Manage Complaint Status Log Function   
Function ID: FR-23   
Description: Administrators and Police Personnel can view, edit, or delete entries in the ComplaintStatusLog to track changes in complaint statuses.   
Input: Valid complaint ID and action (e.g., view, edit, delete).   
Output: Updated ComplaintStatusLog data, management action logged, and notification sent to the Citizen if configured.  
  
1.24 Delete Automated Investigation Record Function   
Function ID: FR-24   
Description: Administrators and Police Personnel can delete an automated investigation record from the system.   
Input: Valid complaint ID and confirmation from the user.   
Output: Deleted AutomatedInvestigation record, complaint status updated, and notification sent to the Citizen and relevant Police Personnel.  
  
1.25 Manage Search Records Function   
Function ID: FR-25   
Description: Administrators and Police Personnel can manage search records by viewing, editing, or deleting them.   
Input: Valid search ID and action (e.g., view, edit, delete).   
Output: Updated or deleted search record, management action logged, and search history updated accordingly.  
  
1.26 Manage Citizen Records Function   
Function ID: FR-26   
Description: Administrators and Police Personnel can manage Citizen records by viewing, editing, or deleting them.   
Input: Valid citizen ID and action (e.g., view, edit, delete).   
Output: Updated or deleted Citizen record, management action logged, and notification sent to the Citizen if configured.  
  
1.27 Manage Police Personnel Records Function   
Function ID: FR-27   
Description: Administrators can manage Police Personnel records by viewing, editing, or deleting them.   
Input: Valid Police Personnel ID and action (e.g., view, edit, delete).   
Output: Updated or deleted Police Personnel record, management action logged, and notification sent to the Police Personnel if configured.  
  
1.28 Manage Administrator Records Function   
Function ID: FR-28   
Description: Administrators can manage other Administrator records by viewing, editing, or deleting them.   
Input: Valid Administrator ID and action (e.g., view, edit, delete).   
Output: Updated or deleted Administrator record, management action logged, and notification sent to the affected Administrator if configured.

# External Description

2. External Interfaces   
This section outlines the external interfaces required for the system to interact with users, hardware, software, and communication channels. These interfaces are essential for supporting the functional requirements and ensuring seamless data exchange and user experience.  
  
2.1 User Interface Output   
The system must provide a user interface for interaction with three types of users: Citizens, Police Personnel, and Administrators. The interface will be implemented through a web-based platform with a responsive design for accessibility across devices.  
  
- \*\*Complaint Registration Interface\*\*: Citizens can submit a new complaint by entering the incident description, location, date, and uploading supporting documents. The interface must also accept the citizen’s ID for verification.   
- \*\*Complaint View Interface\*\*: Police Personnel and Administrators can view detailed complaint information, including the status and associated automated investigation data.   
- \*\*Court Case View Interface\*\*: All users (Citizens, Police Personnel, and Administrators) can view court case details, including related complaint data.   
- \*\*Investigation Progress Interface\*\*: All users can view the progress of an automated investigation, including stages completed, pending actions, and findings.   
- \*\*Search Interface\*\*: Police Personnel and Administrators can search for crime-related records, criminal profiles, and investigation data using various criteria such as keywords, dates, and locations.   
- \*\*User Management Interface\*\*: Administrators can manage user accounts by creating, updating, or deleting user records. This interface includes fields for user roles, contact information, and login credentials.   
- \*\*System Configuration Interface\*\*: Administrators can configure system-wide settings, such as notification preferences, access control rules, and automated investigation parameters.   
- \*\*Log Management Interface\*\*: Administrators and Police Personnel can view, edit, or delete entries in the ComplaintStatusLog and CaseStatusLog.   
- \*\*Notification Interface\*\*: All users can receive notifications about changes in complaint status, court case status, or investigation progress.   
  
2.2 Hardware Interface Output   
The system does not require direct interaction with hardware devices. However, it may be accessed through various hardware platforms, including desktops, laptops, tablets, and mobile phones. The following hardware considerations must be addressed to ensure compatibility:  
  
- \*\*Input Devices\*\*: Support for standard input devices such as keyboards, mice, and touchscreen interfaces for data entry and navigation.   
- \*\*Output Devices\*\*: Compatibility with standard display devices for rendering the user interface and printing complaint or court case details if needed.   
- \*\*Storage Devices\*\*: Optional support for external storage devices to import or export documents (e.g., evidence files or PDF summaries of complaints and court cases).   
  
2.3 Software Interface Output   
The system must interface with the following software components to store, retrieve, and manage data:  
  
- \*\*Complaint Database\*\*: A relational database used to store and manage complaint records. Each complaint record includes the incident description, location, date, supporting documents, and a unique complaint ID. The system must support CRUD operations (Create, Read, Update, Delete) on this database.   
- \*\*Court Case Database\*\*: A relational database to store court case records, including court name, case type, filing date, and involved parties. The system must link court cases to their associated complaint records.   
- \*\*AutomatedInvestigation Database\*\*: A database to store records of automated investigations, including findings, evidence, witness information, and investigation status.   
- \*\*ComplaintStatusLog Database\*\*: A database to log all changes in complaint status, including the date of the change, user who made the change, and the new status.   
- \*\*CaseStatusLog Database\*\*: A database to log all changes in court case status, including the date of the change, user who made the change, and the new status.   
- \*\*User Database\*\*: A database to manage user accounts, including roles (Citizen, Police Personnel, Administrator), login credentials, and contact information.   
- \*\*Search Log Database\*\*: A database to store logs of all search activities performed by Police Personnel and Administrators.   
- \*\*Notification System\*\*: The system must interface with a notification module to send status updates and alerts to users. This may include internal notifications within the system or external communication channels (e.g., email).   
- \*\*Document Management System\*\*: The system must support document uploads and storage for supporting documents, evidence, and investigation notes. The documents must be stored securely and accessible via the complaint or court case records.   
  
2.4 Communication Interface Output   
The system must support communication interfaces for sending notifications, exchanging data, and ensuring secure access to the system.  
  
- \*\*Email Notification Interface\*\*: The system must send email notifications to citizens and police personnel when a complaint or court case status is updated, when an automated investigation is initiated, or when a search is performed. The interface must support secure email transmission and authentication.   
- \*\*User Authentication Interface\*\*: The system must provide a secure login interface for all users, including authentication mechanisms such as username/password, multi-factor authentication (MFA), or role-based access control.   
- \*\*Internal Communication Interface\*\*: Police Personnel and Administrators must be able to send internal messages or escalate cases to other users within the system. This includes status updates and investigation notes.   
- \*\*External API Interface (if applicable)\*\*: The system may integrate with external APIs for data validation, criminal record checks, or court scheduling. If an API is used, it must support secure data exchange and return structured responses (e.g., JSON or XML).   
- \*\*Web Browsing Interface\*\*: The system must be accessible through a web browser using standard HTTP/HTTPS protocols. All data exchanges must be encrypted to ensure security.   
- \*\*Data Export Interface\*\*: The system must allow Police Personnel and Administrators to export data in standard formats (e.g., CSV, Excel, or PDF) for reporting and analysis purposes.   
  
This section ensures that all external interfaces required by the system are clearly defined and categorized, providing developers with a comprehensive understanding of the interactions involved in implementing the system.

# Use Case

Use Case Name: Complaint Registration   
Use Case ID: UC-01   
Actors: Citizen, Police Personnel, Administrator   
Preconditions:   
1. The Citizen has access to the system.   
2. The system is operational and available for complaint submission.   
3. The Citizen has a valid identity for registration.   
  
Postconditions:   
1. The complaint is successfully recorded in the system.   
2. The complaint is assigned for automated investigation.   
3. The Citizen receives a confirmation message and a complaint ID.   
  
Main Flow:   
1. The Citizen logs in to the system.   
2. The Citizen selects the "Register Complaint" option from the main menu.   
3. The system displays a complaint form with fields for details such as incident description, location, date, and supporting documents.   
4. The Citizen fills in the complaint form and submits it.   
5. The system validates the form data and confirms that all required fields are completed.   
6. The system generates a unique complaint ID and stores the complaint in the database.   
7. The system assigns the complaint to an automated investigation process.   
8. The system sends a confirmation message to the Citizen with the complaint ID and estimated processing time.   
9. The Administrator is notified of the new complaint for review.   
  
Alternative Flow:   
1. If the Citizen does not complete all required fields in the complaint form, the system displays an error message and prompts the Citizen to correct the missing information.   
2. If the system fails to generate a complaint ID, the Administrator is alerted to investigate the issue, and the Citizen is notified that the complaint could not be registered.   
3. If the system is unable to assign the complaint to the automated investigation, the Administrator manually assigns the complaint to a relevant department or personnel.  
  
Use Case Name: View Complaint Details   
Use Case ID: UC-02   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has logged into the system.   
2. The complaint exists in the database with a valid complaint ID.   
3. The user has the necessary permissions to view the complaint details.   
  
Postconditions:   
1. The complaint details are displayed to the user.   
2. The system logs the access to the complaint details.   
3. The user has the option to update or escalate the complaint.   
  
Main Flow:   
1. The Police Personnel or Administrator logs in to the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user enters or selects a valid complaint ID from the list.   
4. The system retrieves the complaint details from the database.   
5. The system displays the complaint information, including incident description, location, date, and any supporting documents.   
6. The system shows the current status of the automated investigation if applicable.   
7. The user reviews the displayed information.   
  
Alternative Flow:   
1. If the entered complaint ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to view the complaint, the system denies access and displays a message indicating insufficient rights.   
3. If the system fails to retrieve the complaint details, the Administrator is notified of the error, and the user is informed that the details could not be accessed at this time.  
  
Use Case Name: Update Complaint Status   
Use Case ID: UC-03   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The complaint exists in the system with a valid complaint ID.   
3. The user has the necessary permissions to update the complaint status.   
  
Postconditions:   
1. The complaint status is updated in the system.   
2. The system logs the status update activity.   
3. The Citizen is notified of the updated status via the system.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user selects a complaint from the list using a valid complaint ID.   
4. The system displays the current complaint details and status.   
5. The user selects the "Update Status" option.   
6. The system presents available status options (e.g., "Under Review", "Investigation In Progress", "Resolved", "Escalated").   
7. The user selects a new status and provides an optional comment or reason for the update.   
8. The system saves the updated status and logs the change.   
9. The system sends a notification to the Citizen regarding the new status.   
10. The user is shown a confirmation message that the status was successfully updated.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid, the system displays an error and prompts the user to re-enter a valid ID.   
2. If the user does not have the required permissions to update the status, the system denies the action and displays an access restriction message.   
3. If the system fails to save the updated status, the Administrator is alerted, and the user is notified that the update could not be completed.   
4. If no comment is provided, the system still allows the status update but records it as "No comment provided".  
  
Use Case Name: Delete Complaint Record   
Use Case ID: UC-04   
Actors: Administrator   
Preconditions:   
1. The Administrator has logged into the system.   
2. The complaint record to be deleted exists in the database with a valid complaint ID.   
3. The Administrator has the necessary permissions to delete the complaint record.   
  
Postconditions:   
1. The selected complaint record is permanently removed from the system.   
2. The system logs the deletion activity.   
3. The Citizen and any associated Police Personnel are notified of the deletion if required.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "Complaint Management" section.   
3. The Administrator selects the "Delete Complaint" option.   
4. The system displays a list of existing complaints for selection.   
5. The Administrator selects a valid complaint ID.   
6. The system confirms the selected complaint details before deletion.   
7. The Administrator confirms the deletion.   
8. The system deletes the complaint record from the database.   
9. The system logs the deletion with a timestamp and user ID.   
10. The system sends a notification to the Citizen and relevant Police Personnel (if configured).   
11. The Administrator is shown a confirmation message that the deletion was successful.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or does not exist, the system displays an error message and prompts the Administrator to select a valid ID.   
2. If the Administrator does not have permission to delete the complaint, the system denies access and displays an appropriate message.   
3. If the system fails to delete the complaint record, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the Administrator cancels the deletion during confirmation, the system returns to the complaint list without making any changes.  
  
Use Case Name: Automated Investigation Initiation   
Use Case ID: UC-05   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. A complaint has been registered and is available in the database with a valid complaint ID.   
3. The system is configured to support automated investigation workflows.   
  
Postconditions:   
1. The automated investigation is initiated for the selected complaint.   
2. The system logs the initiation of the investigation.   
3. Relevant Police Personnel are assigned or notified for further action if needed.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user selects a complaint from the list using a valid complaint ID.   
4. The system displays the complaint details and confirms the current status.   
5. The user selects the "Initiate Automated Investigation" option.   
6. The system triggers the automated investigation process, which includes data analysis and pattern recognition.   
7. The system assigns the complaint to an appropriate automated investigation module.   
8. The system updates the complaint status to "Automated Investigation In Progress".   
9. The system logs the action and sends a notification to the relevant Police Personnel.   
10. The user is shown a confirmation message that the investigation has been initiated.   
  
Alternative Flow:   
1. If the complaint is already under investigation, the system displays a message indicating that no further action is required.   
2. If the system fails to initiate the automated investigation, the Administrator is alerted and the user is informed of the issue.   
3. If the selected complaint ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
4. If the user does not have the required permissions to initiate an automated investigation, the system denies the action and displays an access restriction message.  
  
Use Case Name: Modify Investigation Data   
Use Case ID: UC-06   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. A complaint with a valid complaint ID exists in the database and is under automated investigation.   
3. The user has the necessary permissions to modify investigation data.   
  
Postconditions:   
1. The investigation data is successfully updated in the system.   
2. The system logs the modification activity.   
3. The updated status of the complaint is recorded, if applicable.   
4. The Citizen and any relevant Police Personnel are notified of the changes, if configured.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user selects a complaint from the list using a valid complaint ID.   
4. The system displays the complaint details and the current investigation data.   
5. The user selects the "Modify Investigation Data" option.   
6. The system presents editable fields related to the investigation, such as evidence, witness information, or investigation notes.   
7. The user updates the relevant fields and submits the changes.   
8. The system validates the updated data and saves the changes to the database.   
9. The system updates the complaint status, if required.   
10. The system logs the modification and sends a notification to the Citizen and relevant Police Personnel (if configured).   
11. The user is shown a confirmation message that the investigation data has been successfully modified.   
  
Alternative Flow:   
1. If the selected complaint is not under automated investigation, the system displays a message indicating that modifications are not allowed at this stage.   
2. If the user does not have permission to modify the investigation data, the system denies the action and displays an access restriction message.   
3. If the system fails to save the updated investigation data, an error message is shown, and the Administrator is alerted for further investigation.   
4. If no changes are made, the system prompts the user to confirm whether they wish to proceed without making any modifications.   
5. If the system is unable to send notifications, the user is informed, and the Administrator is alerted to manually notify the Citizen or relevant personnel.  
  
Use Case Name: View Investigation Progress   
Use Case ID: UC-07   
Actors: Citizen, Police Personnel, Administrator   
Preconditions:   
1. The Citizen, Police Personnel, or Administrator has logged into the system.   
2. The complaint is registered in the system with a valid complaint ID.   
3. The automated investigation has been initiated for the complaint.   
  
Postconditions:   
1. The current progress of the automated investigation is displayed to the user.   
2. The system logs the access to the investigation progress.   
3. The user may take further actions based on the displayed progress.   
  
Main Flow:   
1. The Citizen, Police Personnel, or Administrator logs into the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user selects the complaint using a valid complaint ID.   
4. The system displays the complaint details, including the current status and progress of the automated investigation.   
5. The system shows any relevant information such as steps completed, pending actions, or investigation findings.   
6. The user reviews the displayed progress.   
7. The system logs the access to the investigation progress.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the complaint has not been assigned to an automated investigation, the system displays a message indicating that no progress is available yet.   
3. If the user does not have permission to view the investigation progress, the system denies access and displays an appropriate message.   
4. If the system fails to retrieve the investigation progress, an error message is shown, and the Administrator is alerted for further investigation.  
  
Use Case Name: Court Case Registration   
Use Case ID: UC-08   
Actors: Administrator, Police Personnel   
Preconditions:   
1. The Administrator or Police Personnel has successfully logged into the system.   
2. A complaint has been registered and is under automated investigation with a valid complaint ID.   
3. The system is configured to support court case registration.   
  
Postconditions:   
1. A court case is successfully created and linked to the complaint in the system.   
2. The system logs the registration of the court case.   
3. The Citizen is notified that the complaint has been escalated to a court case.   
  
Main Flow:   
1. The Administrator or Police Personnel logs into the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user selects a complaint using a valid complaint ID.   
4. The system confirms the complaint is under automated investigation and ready for escalation.   
5. The user selects the "Register Court Case" option.   
6. The system displays a court case registration form with fields such as court name, case type, filing date, and involved parties.   
7. The user fills in the court case details and submits the form.   
8. The system validates the court case data and generates a unique court case ID.   
9. The system links the court case to the complaint and stores the information in the database.   
10. The system logs the action and sends a notification to the Citizen about the court case registration.   
11. The user is shown a confirmation message that the court case was successfully registered.   
  
Alternative Flow:   
1. If the selected complaint is not under automated investigation, the system displays a message that court case registration is not applicable.   
2. If the court case registration form is incomplete or contains invalid data, the system displays an error message and prompts the user to correct the information.   
3. If the system fails to generate a court case ID, the Administrator is alerted, and the user is informed that the registration could not be completed.   
4. If the user does not have permission to register a court case, the system denies the action and displays an access restriction message.   
5. If the system is unable to notify the Citizen, the user is informed and the Administrator is alerted to manually send the notification.  
  
Use Case Name: Update Court Case Status   
Use Case ID: UC-09   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The court case exists in the system and is linked to a valid complaint ID.   
3. The user has the necessary permissions to update the court case status.   
  
Postconditions:   
1. The court case status is updated in the system.   
2. The system logs the update activity.   
3. The Citizen is notified of the court case status change, if configured.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Court Case Management" section.   
3. The user selects the court case using a valid court case ID.   
4. The system displays the court case details, including the current status.   
5. The user selects the "Update Status" option.   
6. The system presents available court case status options (e.g., "Pending", "In Trial", "Closed", "Appealed").   
7. The user selects a new status and optionally provides a reason or comment.   
8. The system saves the updated status and logs the change.   
9. The system sends a notification to the Citizen about the updated court case status, if configured.   
10. The user receives a confirmation message that the court case status has been successfully updated.   
  
Alternative Flow:   
1. If the selected court case ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to update the court case status, the system denies the action and shows an access restriction message.   
3. If the system fails to save the updated court case status, the user is informed of the error, and the Administrator is alerted for further investigation.   
4. If no comment is provided, the system still allows the update and records it as "No comment provided".  
  
Use Case Name: View Court Case Details   
Use Case ID: UC-10   
Actors: Citizen, Police Personnel, Administrator   
Preconditions:   
1. The Citizen, Police Personnel, or Administrator has logged into the system.   
2. The court case exists in the database with a valid court case ID.   
3. The user has the necessary permissions to view the court case details.   
  
Postconditions:   
1. The court case details are displayed to the user.   
2. The system logs the access to the court case details.   
3. The user has the option to take further actions such as updating the court case or viewing related complaints.   
  
Main Flow:   
1. The Citizen, Police Personnel, or Administrator logs into the system.   
2. The user navigates to the "Court Case Management" section.   
3. The user selects a valid court case ID from the list or enters it manually.   
4. The system retrieves the court case details from the database.   
5. The system displays the court case information, including case type, filing date, involved parties, and current status.   
6. The system shows any related complaint details if applicable.   
7. The user reviews the displayed court case information.   
  
Alternative Flow:   
1. If the entered court case ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to view the court case, the system denies access and displays a message indicating insufficient rights.   
3. If the system fails to retrieve the court case details, the user is informed of the issue, and the Administrator is alerted for further investigation.  
  
Use Case Name: Delete Court Case Record   
Use Case ID: UC-11   
Actors: Administrator   
Preconditions:   
1. The Administrator has successfully logged into the system.   
2. The court case to be deleted exists in the system with a valid court case ID.   
3. The Administrator has the required permissions to delete court case records.   
  
Postconditions:   
1. The selected court case record is permanently removed from the system.   
2. The system logs the deletion with a timestamp and user ID.   
3. The Citizen and any associated Police Personnel are notified of the deletion, if configured.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "Court Case Management" section.   
3. The Administrator selects the "Delete Court Case" option.   
4. The system displays a list of court cases for selection.   
5. The Administrator selects a valid court case ID.   
6. The system confirms the court case details before deletion.   
7. The Administrator confirms the deletion request.   
8. The system deletes the court case record from the database.   
9. The system logs the deletion activity.   
10. The system sends a notification to the Citizen and relevant Police Personnel (if configured).   
11. The Administrator is shown a confirmation message that the deletion was successful.   
  
Alternative Flow:   
1. If the selected court case ID is invalid or does not exist, the system displays an error message and prompts the Administrator to re-enter a valid ID.   
2. If the Administrator does not have the required permissions, the system denies the action and displays an access restriction message.   
3. If the system fails to delete the court case record, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the Administrator cancels the deletion during confirmation, the system returns to the court case list without making any changes.  
  
Use Case Name: Search for Crimes   
Use Case ID: UC-12   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The system contains a database of registered complaints and court cases.   
3. The user has the necessary permissions to perform a search for crime-related data.   
  
Postconditions:   
1. Relevant crime data is displayed to the user based on the search criteria.   
2. The system logs the search activity.   
3. The user can take further actions, such as viewing complaint or court case details.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Crime Search" section.   
3. The system provides search options such as keyword search, date range, location, or complaint ID.   
4. The user selects one or more search criteria and submits the query.   
5. The system searches the database for matching crime-related records.   
6. The system displays a list of matching complaints or court cases with summary information.   
7. The user can select a specific record to view more details.   
8. The system logs the search and displays results to the user.   
  
Alternative Flow:   
1. If no matching records are found, the system displays a message indicating no results were found.   
2. If the user does not have permission to perform the search, the system denies access and displays an appropriate message.   
3. If the system fails to retrieve the search results, the user is informed of the issue, and the Administrator is alerted for further investigation.   
4. If the search criteria are incomplete or invalid, the system displays an error message and prompts the user to refine the search.  
  
Use Case Name: Search for Criminals   
Use Case ID: UC-13   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The system contains a database of criminal records or individuals associated with complaints or court cases.   
3. The user has the necessary permissions to perform a search for criminal data.   
  
Postconditions:   
1. Relevant criminal records are displayed to the user based on the search criteria.   
2. The system logs the search activity.   
3. The user can take further actions, such as viewing related complaints or court cases.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Criminal Search" section.   
3. The system provides search options such as name, age range, gender, location, or case ID.   
4. The user selects one or more search criteria and submits the query.   
5. The system searches the database for matching criminal records.   
6. The system displays a list of matching criminals with summary information (e.g., name, age, criminal history).   
7. The user can select a specific criminal to view detailed information.   
8. The system logs the search and displays the criminal details.   
  
Alternative Flow:   
1. If no matching criminals are found, the system displays a message indicating no results were found.   
2. If the user does not have permission to perform the search, the system denies access and displays an appropriate message.   
3. If the system fails to retrieve the search results, the user is informed of the issue, and the Administrator is alerted for further investigation.   
4. If the search criteria are incomplete or invalid, the system displays an error message and prompts the user to refine the search.  
  
Use Case Name: Search for Investigation Records   
Use Case ID: UC-14   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The system contains a database of complaints with associated automated investigation records.   
3. The user has the necessary permissions to search for investigation data.   
  
Postconditions:   
1. Relevant investigation records are displayed to the user based on the search criteria.   
2. The system logs the search activity.   
3. The user can take further actions, such as viewing or modifying the investigation data.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Investigation Search" section.   
3. The system provides search options such as complaint ID, investigation status, date range, or keywords.   
4. The user selects one or more search criteria and submits the query.   
5. The system searches the database for matching investigation records.   
6. The system displays a list of matching investigations with summary details (e.g., complaint ID, status, date initiated).   
7. The user can select a specific investigation to view more detailed information.   
8. The system logs the search and displays the investigation details.   
  
Alternative Flow:   
1. If no matching investigation records are found, the system displays a message indicating no results were found.   
2. If the user does not have permission to perform the search, the system denies access and displays an appropriate message.   
3. If the system fails to retrieve the search results, the user is informed of the issue, and the Administrator is alerted for further investigation.   
4. If the search criteria are incomplete or invalid, the system displays an error message and prompts the user to refine the search.  
  
Use Case Name: Citizen Submit Complaint   
Use Case ID: UC-00   
Actors: Citizen   
Preconditions:   
1. The Citizen has access to the system.   
2. The system is operational and available for complaint submission.   
3. The Citizen has a valid identity for submission.   
  
Postconditions:   
1. The complaint is submitted and stored in the system.   
2. A complaint ID is generated and provided to the Citizen.   
3. The system initiates a log for the submitted complaint.   
  
Main Flow:   
1. The Citizen accesses the system and logs in.   
2. The Citizen navigates to the "Submit Complaint" interface.   
3. The system displays a form with required fields (e.g., incident description, location, date).   
4. The Citizen fills in the form and uploads any supporting documents.   
5. The system validates all required fields and confirms data integrity.   
6. The system generates a unique complaint ID and stores the complaint in the database.   
7. The system sends a confirmation message to the Citizen, including the complaint ID and estimated processing time.   
8. The system logs the submission activity for tracking and auditing.   
  
Alternative Flow:   
1. If the Citizen fails to complete required fields, the system displays an error and prompts for correction.   
2. If the system fails to generate a complaint ID, the Administrator is notified, and the Citizen is informed of the failure.   
3. If the complaint submission is interrupted due to system error, the system retries or displays an error message to the Citizen.  
  
Use Case Name: Citizen View Complaint Status   
Use Case ID: UC-15   
Actors: Citizen   
Preconditions:   
1. The Citizen has successfully logged into the system.   
2. The complaint has been previously registered and is stored in the system with a valid complaint ID.   
3. The system supports the functionality for viewing the status of a complaint.   
  
Postconditions:   
1. The current status of the complaint is displayed to the Citizen.   
2. The system logs the Citizen's access to the complaint status.   
3. The Citizen is informed about any updates in the complaint or automated investigation process.   
  
Main Flow:   
1. The Citizen logs into the system.   
2. The Citizen navigates to the "View Complaint Status" section.   
3. The system displays a list of the Citizen's previously submitted complaints.   
4. The Citizen selects a complaint by entering or clicking on a valid complaint ID.   
5. The system retrieves the current status of the selected complaint.   
6. The system displays the complaint status, along with any additional information such as the current stage of the automated investigation, expected resolution time, or recent updates.   
7. The Citizen reviews the displayed complaint status.   
8. The system logs the viewing activity.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or not associated with the Citizen, the system displays an error message and prompts for a valid ID.   
2. If the system is unable to retrieve the complaint status, the Citizen is notified of the issue, and the Administrator is alerted for investigation.   
3. If the complaint is still being processed and no status is available, the system informs the Citizen that the complaint is under review.  
  
Use Case Name: Police Personnel Manage Complaints   
Use Case ID: UC-16   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The complaint exists in the system and is associated with a valid complaint ID.   
3. The user has the necessary permissions to manage complaint records.   
  
Postconditions:   
1. The complaint is either updated, escalated, or otherwise managed in the system.   
2. The system logs the management activity with a timestamp and user ID.   
3. The Citizen is notified of the changes or actions taken, if configured.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Complaint Management" section.   
3. The user selects a complaint by entering or selecting a valid complaint ID.   
4. The system displays the complaint details and its current status.   
5. The user chooses an action to perform on the complaint, such as updating the status, escalating the case, or adding notes.   
6. The system processes the selected action and updates the complaint accordingly.   
7. The system logs the action and sends a notification to the Citizen, if configured.   
8. The user is shown a confirmation message that the complaint has been successfully managed.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have the required permissions to manage the complaint, the system denies the action and displays an access restriction message.   
3. If the system fails to update or manage the complaint, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user cancels the action during the process, the system returns to the complaint list without making any changes.  
  
Use Case Name: Police Personnel Manage Investigations   
Use Case ID: UC-17   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The complaint is registered in the system and is under automated investigation with a valid complaint ID.   
3. The user has the necessary permissions to manage the automated investigation.   
  
Postconditions:   
1. The automated investigation is either updated, paused, or escalated based on user action.   
2. The system logs the management activity with a timestamp and user ID.   
3. The Citizen is notified of the changes or actions taken, if configured.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Investigation Management" section.   
3. The user selects an ongoing automated investigation by entering or selecting a valid complaint ID.   
4. The system displays the current investigation status, progress, and relevant data.   
5. The user chooses an action to manage the investigation (e.g., update findings, pause investigation, escalate to manual review).   
6. The system processes the selected action and updates the investigation accordingly.   
7. The system logs the action and sends a notification to the Citizen, if configured.   
8. The user is shown a confirmation message that the investigation has been successfully managed.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or not under automated investigation, the system displays an error message and prompts the user to select a valid ID.   
2. If the user does not have permission to manage the investigation, the system denies the action and displays an access restriction message.   
3. If the system fails to process the management action, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user cancels the action during the process, the system returns to the investigation list without making any changes.  
  
Use Case Name: Administrator Manage Users   
Use Case ID: UC-18   
Actors: Administrator   
Preconditions:   
1. The Administrator has successfully logged into the system.   
2. The system contains a user database with registered users (Citizen, Police Personnel, and other Administrators).   
3. The Administrator has the necessary permissions to manage user accounts.   
  
Postconditions:   
1. The user account is either created, updated, or deleted in the system.   
2. The system logs all user management activities with a timestamp and Administrator ID.   
3. The affected user receives a notification if applicable.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "User Management" section.   
3. The system displays a list of existing users, including their roles and status.   
4. The Administrator selects an action (Create, Update, or Delete) for a specific user or a new user.   
5. If creating a new user, the Administrator fills in the required user details (e.g., name, role, contact information).   
6. The system validates the input data and confirms the user's role and permissions.   
7. The system saves the user information to the database and generates a unique user ID.   
8. The system logs the action and sends a notification to the user (if configured).   
9. The Administrator receives a confirmation message that the action was successful.   
  
Alternative Flow:   
1. If the user details are incomplete or invalid, the system displays an error message and prompts the Administrator to correct the information.   
2. If the selected user does not exist, the system displays an error message and prompts the Administrator to enter a valid user ID.   
3. If the system fails to save the user information, the Administrator is alerted, and an error message is displayed.   
4. If the Administrator does not have the required permissions to perform the action, the system denies the request and displays an access restriction message.   
5. If the system is unable to send notifications to the user, the Administrator is alerted to manually handle the communication.  
  
Use Case Name: Administrator Configure System Settings   
Use Case ID: UC-19   
Actors: Administrator   
Preconditions:   
1. The Administrator has successfully logged into the system.   
2. The system has a configuration interface accessible to the Administrator.   
3. The system supports the configuration of settings such as user roles, automated investigation rules, or notification preferences.   
  
Postconditions:   
1. The system settings are updated according to the Administrator's configuration.   
2. The system logs the configuration changes with a timestamp and Administrator ID.   
3. The updated settings are applied to the system operations.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "System Configuration" section.   
3. The system displays a list of configurable settings (e.g., user permissions, investigation workflow, notification settings).   
4. The Administrator selects a setting to configure.   
5. The system opens the configuration interface for the selected setting.   
6. The Administrator makes the necessary changes (e.g., modifies a user role, adjusts automated investigation rules).   
7. The Administrator submits the configuration changes.   
8. The system validates the configuration and applies the changes.   
9. The system logs the configuration update.   
10. The Administrator is shown a confirmation message that the settings have been successfully updated.   
  
Alternative Flow:   
1. If the configuration data is invalid or incomplete, the system displays an error message and prompts the Administrator to correct the input.   
2. If the Administrator does not have permission to modify the system settings, the system denies the action and displays an access restriction message.   
3. If the system fails to apply the configuration changes, the Administrator is alerted, and an error message is displayed.   
4. If the Administrator cancels the configuration during the process, the system returns to the configuration list without making any changes.  
  
Use Case Name: Manage Investigation Progress   
Use Case ID: UC-20   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The complaint is registered in the system and is under automated investigation with a valid complaint ID.   
3. The user has the necessary permissions to manage or update the investigation progress.   
  
Postconditions:   
1. The investigation progress is updated in the system.   
2. The system logs the modification of the investigation progress with a timestamp and user ID.   
3. The Citizen is notified of the updated investigation progress, if configured.   
4. The complaint status is adjusted to reflect the new progress, if applicable.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Investigation Progress Management" section.   
3. The user selects a complaint by entering or selecting a valid complaint ID.   
4. The system displays the current investigation progress, including stages completed, pending actions, and findings.   
5. The user chooses an action to modify the investigation progress (e.g., add progress notes, mark a stage as completed, or update findings).   
6. The user inputs the new progress details and submits the changes.   
7. The system validates the input and updates the investigation progress in the database.   
8. The system logs the action and sends a notification to the Citizen about the updated progress, if configured.   
9. The system updates the complaint status to reflect the changes in the investigation process.   
10. The user is shown a confirmation message that the investigation progress has been successfully updated.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or not under automated investigation, the system displays an error message and prompts the user to select a valid ID.   
2. If the user does not have the required permissions to manage the investigation progress, the system denies the action and displays an access restriction message.   
3. If the system fails to save the updated investigation progress, the user is informed of the error, and the Administrator is alerted for further investigation.   
4. If the user cancels the action during the process, the system returns to the investigation progress list without making any changes.   
5. If the system is unable to send a notification to the Citizen, the user is informed, and the Administrator is alerted to manually notify the Citizen.  
  
Use Case Name: Manage Case Status Log   
Use Case ID: UC-21   
Actors: Administrator, Police Personnel   
Preconditions:   
1. The Administrator or Police Personnel has successfully logged into the system.   
2. The complaint or court case is registered in the system and has a valid complaint ID or court case ID.   
3. The system maintains a Case Status Log for tracking changes in complaint or court case statuses.   
4. The user has the necessary permissions to view, edit, or delete entries in the Case Status Log.   
  
Postconditions:   
1. The Case Status Log is updated or modified in the system.   
2. The system logs the management activity with a timestamp and user ID.   
3. The Citizen or relevant personnel are notified of any changes in the Case Status Log, if configured.   
  
Main Flow:   
1. The Administrator or Police Personnel logs into the system.   
2. The user navigates to the "Case Status Log Management" section.   
3. The system displays a list of complaints or court cases for which the Case Status Log is available.   
4. The user selects a complaint or court case by entering or selecting a valid complaint ID or court case ID.   
5. The system retrieves and displays the Case Status Log entries for the selected case, including the date, time, user who made the change, and the status change details.   
6. The user selects an action to perform on the Case Status Log (e.g., view log, edit log entry, delete log entry).   
7. If editing or deleting a log entry, the user confirms the action with additional verification.   
8. The system processes the selected action and updates the Case Status Log accordingly.   
9. The system logs the management action with a timestamp and user ID.   
10. The user receives a confirmation message that the Case Status Log has been successfully managed.   
  
Alternative Flow:   
1. If the selected complaint or court case ID is invalid, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to manage the Case Status Log, the system denies the action and displays an access restriction message.   
3. If the system fails to retrieve the Case Status Log, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user selects a log entry that cannot be edited or deleted (e.g., system-generated or historical log entries), the system displays a message explaining the restriction.   
5. If the system is unable to log the management action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Manage Complaint Status Log   
Use Case ID: UC-22   
Actors: Administrator, Police Personnel   
Preconditions:   
1. The Administrator or Police Personnel has successfully logged into the system.   
2. The complaint is registered in the system and has a valid complaint ID.   
3. The system maintains a Complaint Status Log for tracking changes in the complaint's status.   
4. The user has the necessary permissions to view, edit, or delete entries in the Complaint Status Log.   
  
Postconditions:   
1. The Complaint Status Log is updated or modified in the system.   
2. The system logs the management activity with a timestamp and user ID.   
3. The Citizen or relevant personnel are notified of any changes in the Complaint Status Log, if configured.   
  
Main Flow:   
1. The Administrator or Police Personnel logs into the system.   
2. The user navigates to the "Complaint Status Log Management" section.   
3. The system displays a list of complaints for which the Complaint Status Log is available.   
4. The user selects a complaint by entering or selecting a valid complaint ID.   
5. The system retrieves and displays the Complaint Status Log entries for the selected complaint, including the date, time, user who made the change, and the status update details.   
6. The user selects an action to perform on the Complaint Status Log (e.g., view log, edit log entry, delete log entry).   
7. If editing or deleting a log entry, the user confirms the action with additional verification.   
8. The system processes the selected action and updates the Complaint Status Log accordingly.   
9. The system logs the management action with a timestamp and user ID.   
10. The user receives a confirmation message that the Complaint Status Log has been successfully managed.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to manage the Complaint Status Log, the system denies the action and displays an access restriction message.   
3. If the system fails to retrieve the Complaint Status Log, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user selects a log entry that cannot be edited or deleted (e.g., system-generated or historical log entries), the system displays a message explaining the restriction.   
5. If the system is unable to log the management action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Manage System Settings   
Use Case ID: UC-23   
Actors: Administrator   
  
Preconditions:   
1. The Administrator has successfully logged into the system.   
2. The system has a dedicated interface for managing system-wide settings.   
3. The system supports the configuration of settings such as system language, notification preferences, access control rules, and automated investigation parameters.   
  
Postconditions:   
1. The system settings are updated according to the Administrator's configuration.   
2. The system logs the configuration changes with a timestamp and Administrator ID.   
3. The updated settings are applied to the system and affect the behavior of all users accordingly.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "System Settings Management" section.   
3. The system displays a categorized list of available settings (e.g., General Settings, Notification Settings, Investigation Rules, Security Settings).   
4. The Administrator selects a specific category or setting to configure.   
5. The system opens the configuration interface for the selected setting.   
6. The Administrator modifies the settings as required (e.g., enables/disables automated investigation, sets notification channels, updates access control policies).   
7. The Administrator submits the updated settings.   
8. The system validates the input and applies the changes to the system configuration.   
9. The system logs the configuration update, including the Administrator ID and the timestamp.   
10. The system applies the new settings to relevant functionalities.   
11. The Administrator is shown a confirmation message that the system settings have been successfully updated.   
  
Alternative Flow:   
1. If the Administrator does not have the required permissions to modify system settings, the system denies the action and displays an access restriction message.   
2. If the configuration data is invalid or incomplete, the system displays an error message and prompts the Administrator to correct the input.   
3. If the system fails to apply the configuration changes, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the Administrator cancels the configuration during the process, the system returns to the settings list without making any changes.   
5. If the system is unable to log the configuration action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Delete Automated Investigation Record   
Use Case ID: UC-24   
Actors: Administrator, Police Personnel   
  
Preconditions:   
1. The Administrator or Police Personnel has successfully logged into the system.   
2. An automated investigation record exists in the system and is associated with a valid complaint ID.   
3. The user has the necessary permissions to delete automated investigation records.   
  
Postconditions:   
1. The selected automated investigation record is permanently removed from the system.   
2. The system logs the deletion activity with a timestamp and user ID.   
3. The complaint status is updated to reflect the removal of the automated investigation.   
4. The Citizen and any associated Police Personnel are notified of the deletion, if configured.   
  
Main Flow:   
1. The Administrator or Police Personnel logs into the system.   
2. The user navigates to the "Automated Investigation Management" section.   
3. The system displays a list of automated investigations for selection.   
4. The user selects a valid complaint ID associated with an automated investigation.   
5. The system confirms the details of the selected automated investigation.   
6. The user confirms the deletion of the automated investigation record.   
7. The system deletes the automated investigation record from the database.   
8. The system updates the complaint status to "Investigation Deleted" or similar.   
9. The system logs the deletion action with a timestamp and user ID.   
10. The system sends a notification to the Citizen and any relevant Police Personnel (if configured).   
11. The user is shown a confirmation message that the automated investigation record has been successfully deleted.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or does not correspond to an automated investigation, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have the required permissions to delete the automated investigation record, the system denies the action and displays an access restriction message.   
3. If the system fails to delete the automated investigation record, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the deletion is canceled during confirmation, the system returns to the investigation list without making any changes.   
5. If the system is unable to send notifications to the Citizen or Police Personnel, the user is informed, and the Administrator is alerted to manually handle the communication.  
  
Use Case Name: Manage Search Records   
Use Case ID: UC-25   
Actors: Administrator, Police Personnel   
  
Preconditions:   
1. The Administrator or Police Personnel has successfully logged into the system.   
2. The system contains a database of search records related to complaints, court cases, criminals, or investigations.   
3. The user has the necessary permissions to view, edit, or delete search records.   
  
Postconditions:   
1. The search records are updated, viewed, or deleted according to the user's action.   
2. The system logs the management activity of the search records with a timestamp and user ID.   
3. The search history remains accurate and reflects the latest changes.   
  
Main Flow:   
1. The Administrator or Police Personnel logs into the system.   
2. The user navigates to the "Search Record Management" section.   
3. The system displays a list of all search records, including details such as search type (e.g., crime, criminal, investigation), search criteria, and the user who performed the search.   
4. The user selects a specific search record by entering or selecting a valid search ID.   
5. The system retrieves and displays the selected search record with all associated details.   
6. The user chooses an action to perform on the search record (e.g., view, edit, delete).   
7. If editing or deleting, the user confirms the action with additional verification.   
8. The system processes the selected action and updates the search record accordingly.   
9. The system logs the management action with a timestamp and user ID.   
10. The user is shown a confirmation message that the search record has been successfully managed.   
  
Alternative Flow:   
1. If the selected search ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to manage the search records, the system denies the action and displays an access restriction message.   
3. If the system fails to retrieve the search records, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user selects a search record that cannot be edited or deleted (e.g., system-generated or historical search records), the system displays a message explaining the restriction.   
5. If the system is unable to log the management action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Manage Citizen Records   
Use Case ID: UC-26   
Actors: Administrator, Police Personnel   
  
Preconditions:   
1. The Administrator or Police Personnel has successfully logged into the system.   
2. The system contains a database of registered Citizen records.   
3. The user has the necessary permissions to view, edit, or delete Citizen records.   
  
Postconditions:   
1. The Citizen record is updated, viewed, or deleted according to the user's action.   
2. The system logs the management activity of the Citizen record with a timestamp and user ID.   
3. The Citizen is notified of any changes to their record, if configured.   
  
Main Flow:   
1. The Administrator or Police Personnel logs into the system.   
2. The user navigates to the "Citizen Management" section.   
3. The system displays a list of registered Citizen records, including their basic information, complaint history, and status.   
4. The user selects a specific Citizen record by entering or selecting a valid Citizen ID.   
5. The system retrieves and displays the selected Citizen's details, including personal information, submitted complaints, and related court cases.   
6. The user chooses an action to perform on the Citizen record (e.g., view, edit, delete).   
7. If editing or deleting, the user confirms the action with additional verification.   
8. The system processes the selected action and updates the Citizen record accordingly.   
9. The system logs the management action with a timestamp and user ID.   
10. If the action involves deletion or significant modification, the system sends a notification to the Citizen, if configured.   
11. The user is shown a confirmation message that the Citizen record has been successfully managed.   
  
Alternative Flow:   
1. If the selected Citizen ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the user does not have permission to manage the Citizen record, the system denies the action and displays an access restriction message.   
3. If the system fails to retrieve the Citizen record, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user selects a record that cannot be edited or deleted (e.g., protected or system-generated records), the system displays a message explaining the restriction.   
5. If the system is unable to log the management action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Manage Police Personnel Records   
Use Case ID: UC-27   
Actors: Administrator   
  
Preconditions:   
1. The Administrator has successfully logged into the system.   
2. The system contains a database of registered Police Personnel records.   
3. The user has the necessary permissions to view, edit, or delete Police Personnel records.   
  
Postconditions:   
1. The Police Personnel record is updated, viewed, or deleted according to the Administrator's action.   
2. The system logs the management activity of the Police Personnel record with a timestamp and Administrator ID.   
3. The Police Personnel is notified of any changes to their record, if configured.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "Police Personnel Management" section.   
3. The system displays a list of registered Police Personnel records, including their basic information, assigned roles, and activity history.   
4. The Administrator selects a specific Police Personnel record by entering or selecting a valid Police Personnel ID.   
5. The system retrieves and displays the selected Police Personnel's details, including personal information, role, department, and any associated complaints or investigations.   
6. The Administrator chooses an action to perform on the Police Personnel record (e.g., view, edit, delete).   
7. If editing or deleting, the Administrator confirms the action with additional verification.   
8. The system processes the selected action and updates the Police Personnel record accordingly.   
9. The system logs the management action with a timestamp and Administrator ID.   
10. If the action involves deletion or significant modification, the system sends a notification to the Police Personnel, if configured.   
11. The Administrator is shown a confirmation message that the Police Personnel record has been successfully managed.   
  
Alternative Flow:   
1. If the selected Police Personnel ID is invalid or does not exist, the system displays an error message and prompts the Administrator to re-enter a valid ID.   
2. If the Administrator does not have permission to manage the Police Personnel record, the system denies the action and displays an access restriction message.   
3. If the system fails to retrieve the Police Personnel record, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user selects a record that cannot be edited or deleted (e.g., active accounts or system-restricted personnel), the system displays a message explaining the restriction.   
5. If the system is unable to log the management action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Manage Administrator Records   
Use Case ID: UC-28   
Actors: Administrator   
  
Preconditions:   
1. The Administrator has successfully logged into the system.   
2. The system contains a database of registered Administrator records.   
3. The user has the necessary permissions to view, edit, or delete other Administrator records.   
  
Postconditions:   
1. The Administrator record is updated, viewed, or deleted according to the user's action.   
2. The system logs the management activity of the Administrator record with a timestamp and the ID of the performing Administrator.   
3. The affected Administrator is notified of any changes to their record, if configured.   
  
Main Flow:   
1. The Administrator logs into the system.   
2. The Administrator navigates to the "Administrator Management" section.   
3. The system displays a list of registered Administrator records, including their basic information, roles, and access levels.   
4. The Administrator selects a specific Administrator record by entering or selecting a valid Administrator ID.   
5. The system retrieves and displays the selected Administrator's details, including personal information, assigned roles, and activity history.   
6. The Administrator chooses an action to perform on the selected record (e.g., view, edit, delete).   
7. If editing or deleting, the Administrator confirms the action with additional verification.   
8. The system processes the selected action and updates the Administrator record accordingly.   
9. The system logs the management action with a timestamp and the ID of the performing Administrator.   
10. If the action involves deletion or significant modification, the system sends a notification to the affected Administrator, if configured.   
11. The Administrator is shown a confirmation message that the selected Administrator record has been successfully managed.   
  
Alternative Flow:   
1. If the selected Administrator ID is invalid or does not exist, the system displays an error message and prompts the user to re-enter a valid ID.   
2. If the Administrator does not have permission to manage another Administrator's record (e.g., attempting to delete their own account or a higher-privileged account), the system denies the action and displays an access restriction message.   
3. If the system fails to retrieve the Administrator record, an error message is shown, and the Administrator is alerted for further investigation.   
4. If the user selects a record that cannot be edited or deleted (e.g., system-restricted accounts or active users), the system displays a message explaining the restriction.   
5. If the system is unable to log the management action, the Administrator is notified, and the user is informed of the issue.  
  
Use Case Name: Manage Investigation Progress   
Use Case ID: UC-29   
Actors: Police Personnel, Administrator   
Preconditions:   
1. The Police Personnel or Administrator has successfully logged into the system.   
2. The complaint is registered in the system and is under automated investigation with a valid complaint ID.   
3. The user has the necessary permissions to manage or update the investigation progress.   
  
Postconditions:   
1. The investigation progress is updated in the system.   
2. The system logs the modification of the investigation progress with a timestamp and user ID.   
3. The Citizen is notified of the updated investigation progress, if configured.   
4. The complaint status is adjusted to reflect the new progress, if applicable.   
  
Main Flow:   
1. The Police Personnel or Administrator logs into the system.   
2. The user navigates to the "Investigation Progress Management" section.   
3. The user selects a complaint by entering or selecting a valid complaint ID.   
4. The system displays the current investigation progress, including stages completed, pending actions, and findings.   
5. The user chooses an action to modify the investigation progress (e.g., add progress notes, mark a stage as completed, or update findings).   
6. The user inputs the new progress details and submits the changes.   
7. The system validates the input and updates the investigation progress in the database.   
8. The system logs the action and sends a notification to the Citizen about the updated progress, if configured.   
9. The system updates the complaint status to reflect the changes in the investigation process.   
10. The user is shown a confirmation message that the investigation progress has been successfully updated.   
  
Alternative Flow:   
1. If the selected complaint ID is invalid or not under automated investigation, the system displays an error message and prompts the user to select a valid ID.   
2. If the user does not have the required permissions to manage the investigation progress, the system denies the action and displays an access restriction message.   
3. If the system fails to save the updated investigation progress, the user is informed of the error, and the Administrator is alerted for further investigation.   
4. If the user cancels the action during the process, the system returns to the investigation progress list without making any changes.   
5. If the system is unable to send a notification to the Citizen, the user is informed, and the Administrator is alerted to manually notify the Citizen.