项目文档

# 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.

# External Description

2. External Interfaces  
  
2.1 User Interface  
  
The user interface of the system supports interactions between the system and three types of users: citizens, police personnel, and administrators. The interface includes various screens and input forms for data entry and viewing case details.  
  
- \*\*Complaint Submission Screen\*\*: Citizens can submit complaints by entering the nature of the complaint, the date and time of the incident, the location, and a detailed description. They may also upload optional supporting documents. The system will generate a unique complaint ID and display a confirmation message to the user.  
- \*\*Case Management Interface\*\*: Police personnel can update investigation and court case statuses, add notes, and attach evidence. This interface includes forms for entering and modifying case details, viewing case progress, and managing case-complaint links. When sensitive data is accessed, the system will log the activity for audit purposes.  
- \*\*Administrative Interface\*\*: Administrators can configure system settings, manage user roles and permissions, and view access logs and data integrity reports. This interface includes tools for modifying system-wide security policies, notification preferences, and access control rules. Any changes made are logged for audit purposes.  
- \*\*Case Tracking Interface\*\*: Both police personnel and citizens can use this interface to view the progress of an investigation or court case, including status updates and timelines. The system will log any access to sensitive data.  
- \*\*User Profile Interface\*\*: Police personnel and administrators can view and update personal and contact information of citizens and police personnel. This includes input forms for updating addresses, contact details, and other personal information. When sensitive data is accessed, the system will log the activity.  
- \*\*Criminal Record Interface\*\*: Police personnel can add, modify, or delete criminal records. This includes forms for entering criminal information (name, age, offense description), evidence, and associated case IDs. All changes are linked to the relevant investigation or court case and logged for audit purposes.  
- \*\*Search and Filtering Interface\*\*: This interface allows users to search for and filter data by various criteria, such as case IDs, citizen IDs, or time ranges. It supports both basic and advanced search options and logs activity when sensitive data is accessed.  
  
2.2 Hardware Interface  
  
The system does not have direct hardware interfaces. It is designed to operate on standard computing hardware, such as servers, desktop computers, and mobile devices, and does not require any specialized hardware for its core functionalities. However, it may interact indirectly with hardware through external systems such as court case management systems or public notification services.  
  
2.3 Software Interface  
  
The system interacts with the following external software components and data sources:  
  
- \*\*Database System\*\*: The system stores all user data, case data, and configuration settings in a database. This includes complaint records, investigation cases, court cases, criminal records, and access logs. The database supports queries and updates through SQL or NoSQL interfaces, depending on the implementation.  
- \*\*Authentication and Authorization System\*\*: The system integrates with an authentication and authorization service to manage user roles and access rights. This includes assigning unique IDs to users, managing login credentials, and enforcing access control policies.  
- \*\*Email Notification Service\*\*: The system sends confirmation and notification messages via email. For example, when a complaint is registered, the system sends a confirmation message to the citizen. When a case is updated, the system notifies relevant stakeholders. The email service supports standard SMTP protocols or REST APIs for message delivery.  
- \*\*Court Case Management System\*\*: The system exchanges data with a court case management system to maintain synchronization between court cases and related investigations or complaints. This includes updating court case statuses, timelines, and legal documents. The interface supports API calls for data exchange and synchronization.  
- \*\*Audit Logging System\*\*: The system logs all user activities, data modifications, and integrity checks for audit purposes. This includes logs of user access, case updates, criminal record changes, and system configuration modifications. The audit logs are stored in a secure database and may be exported in standard formats (e.g., CSV, JSON) for review.  
- \*\*Public Portal or Mobile Application\*\*: The system may be accessed via a public portal or mobile application for citizens to submit complaints and track case progress. These applications interface with the system through REST APIs and display data in a user-friendly format.  
- \*\*Document Management System\*\*: The system supports the storage and retrieval of supporting documents, such as evidence files or legal documents. These documents are stored in a document management system, and the system provides an interface for uploading, viewing, and managing them.  
  
2.4 Communication Interface  
  
The system communicates with external systems and users through the following methods:  
  
- \*\*Web-Based Communication\*\*: The system is accessible via web browsers and supports HTTP/HTTPS protocols. It uses REST APIs for data exchange between the front-end and back-end components. This allows citizens, police personnel, and administrators to interact with the system from any device with a web browser.  
- \*\*Email Communication\*\*: The system sends notifications and confirmation messages to users via email. It uses standard email protocols (e.g., SMTP) or third-party email services to deliver these messages. Emails are sent in plain text or HTML format, depending on the content and user preferences.  
- \*\*API Communication\*\*: The system communicates with external systems (e.g., court case management systems, authentication services) via API calls. These APIs support JSON or XML data formats and are secured using standard authentication and encryption methods.  
- \*\*Mobile Application Communication\*\*: If the system is accessed via a mobile application, it uses secure communication protocols (e.g., HTTPS) to exchange data with the back-end. The mobile application may also use push notifications to alert users of case updates or system messages.  
- \*\*Data Export Communication\*\*: The system allows administrators to export data, such as access logs or data integrity reports, in standard formats (e.g., CSV, PDF). These exports are triggered via the administrative interface and delivered to the user via download or email.  
  
This section defines all external interfaces necessary for the system to function as described in the functional requirements. Each interface is clearly categorized and described, ensuring that developers can implement the system correctly and efficiently.

# Use Case

Use Case Name: Register Complaint   
Use Case ID: UC-01   
Actors: Citizen, Police Personnel, System   
Preconditions:   
- The citizen has access to the system interface.   
- The citizen has a valid account and is logged in.   
- The system is operational and accessible.   
  
Postconditions:   
- The complaint is successfully recorded in the system.   
- A unique complaint ID is assigned to the complaint.   
- The complaint is assigned to an appropriate police personnel for investigation.   
- The citizen receives a confirmation message with the complaint details.   
  
Main Flow:   
1. The citizen selects the "Register Complaint" option from the main menu.   
2. The system displays a complaint registration form.   
3. The citizen fills in the required details, such as the nature of the complaint, date and time of the incident, location, and a detailed description.   
4. The citizen uploads any supporting documents or evidence (if applicable).   
5. The citizen submits the complaint form.   
6. The system validates the form data and confirms submission.   
7. The system generates a unique complaint ID and assigns the complaint to an investigation case.   
8. The system sends a confirmation message to the citizen, including the complaint ID and estimated response time.   
9. The system notifies the assigned police personnel about the new complaint.   
  
Alternative Flow:   
1. If the citizen does not have a valid account, the system prompts them to register or log in before proceeding.   
2. If the submitted form contains incomplete or invalid data, the system displays an error message and allows the citizen to correct the information.   
3. If no police personnel are available to handle the complaint, the system logs the complaint in a queue and notifies the administrator for intervention.   
4. If the system encounters an error during submission, it displays an error message and suggests retrying the submission later.  
  
Use Case Name: Manage Investigation   
Use Case ID: UC-02   
Actors: Police Personnel, System, Administrator, Court Case   
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- The complaint is already registered and assigned to an investigation case.   
- The system is operational and accessible.   
  
Postconditions:   
- The investigation case is updated with new information or status.   
- Relevant updates are recorded in the system and linked to the complaint.   
- Notifications are sent to involved parties (e.g., citizen, court case, or administrator).   
- The investigation data remains secure and compliant with access control policies.   
  
Main Flow:   
1. The police personnel selects the "Manage Investigation" option from the case dashboard.   
2. The system displays the investigation case details, including the associated complaint, current status, and evidence.   
3. The police personnel updates the investigation status, adds notes, or attaches new evidence.   
4. The system validates the input and saves the updates to the investigation case.   
5. The system links the updates to the corresponding complaint and court case (if applicable).   
6. The system sends a notification to the citizen with the latest investigation status.   
7. The system logs the changes for data integrity and audit purposes.   
  
Alternative Flow:   
1. If the police personnel lacks the required permissions, the system displays an access denied message.   
2. If the system detects invalid or inconsistent data during validation, it prompts the user to correct the input.   
3. If a court case is linked to the investigation and there is a status change, the system notifies the court case handler.   
4. If the system is unable to save the changes due to a technical error, it displays an error message and suggests retrying the action.  
  
Use Case Name: View Investigation Details   
Use Case ID: UC-03   
Actors: Police Personnel, System, Citizen, Administrator   
  
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- An investigation case must exist in the system and be associated with a registered complaint.   
- The system is operational and accessible.   
  
Postconditions:   
- The police personnel can view detailed information about the investigation.   
- The system ensures data integrity and access control during the viewing process.   
- If sensitive information is accessed, the system logs the activity for audit purposes.   
  
Main Flow:   
1. The police personnel selects the "View Investigation Details" option from the case list or dashboard.   
2. The system prompts the user to enter or select an investigation case ID.   
3. The system retrieves and displays all relevant details of the selected investigation, including complaint information, current status, assigned personnel, evidence, and notes.   
4. The police personnel reviews the information and may request additional details from the system.   
5. The system displays the requested information or prompts for clarification if the query is ambiguous.   
  
Alternative Flow:   
1. If the case ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the police personnel does not have permission to view the case, the system displays an access denied message and logs the unauthorized access attempt.   
3. If the system is unable to retrieve the case details due to a technical error, it displays an error message and suggests retrying the request.   
4. If the citizen requests to view the investigation status, the system provides limited information based on the citizen's access rights and logs the access.  
  
Use Case Name: Update Investigation Status   
Use Case ID: UC-04   
Actors: Police Personnel, System, Administrator, Court Case   
  
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- An investigation case must exist in the system and be associated with a registered complaint.   
- The system is operational and accessible.   
  
Postconditions:   
- The investigation status is updated in the system.   
- The update is linked to the relevant complaint and court case (if applicable).   
- Notifications are sent to the citizen and court case handler.   
- The system ensures data integrity and access control during the update process.   
  
Main Flow:   
1. The police personnel selects the "Update Investigation Status" option from the case dashboard.   
2. The system displays the current status and allows the user to select a new status (e.g., "Under Review", "Investigation Completed", "Pending Court Action").   
3. The police personnel selects the new status and optionally adds notes or attaches new documents.   
4. The system validates the input and saves the updated status and any additional information.   
5. The system links the update to the relevant complaint and court case.   
6. The system sends a notification to the citizen with the updated status.   
7. If applicable, the system notifies the court case handler of the change.   
8. The system logs the update for audit and data integrity purposes.   
  
Alternative Flow:   
1. If the selected status is invalid or not supported, the system displays an error and prompts the user to choose a valid option.   
2. If the police personnel lacks the required permissions to update the status, the system displays an access denied message and logs the attempt.   
3. If the system encounters an error while saving the update, it displays an error message and suggests retrying the action.   
4. If the court case is linked and the status change requires administrative approval, the system notifies the administrator for review.  
  
Use Case Name: Add Criminal Record   
Use Case ID: UC-05   
Actors: Police Personnel, System, Administrator   
  
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- The system is operational and accessible.   
- A valid investigation case or court case must exist in the system to link the criminal record.   
  
Postconditions:   
- The criminal record is successfully added to the system.   
- The criminal record is associated with the appropriate investigation or court case.   
- The system ensures data integrity and access control for the new record.   
- Notifications are sent to relevant stakeholders if required.   
  
Main Flow:   
1. The police personnel selects the "Add Criminal Record" option from the case management menu.   
2. The system displays a form for entering criminal record details, including the individual's information, offense description, and evidence.   
3. The police personnel fills in the required information and selects the associated investigation or court case.   
4. The police personnel uploads any supporting documents or evidence.   
5. The police personnel submits the form.   
6. The system validates the input data and confirms the submission.   
7. The system generates a unique criminal record ID and stores the record in the database.   
8. The system links the criminal record to the selected investigation or court case.   
9. The system sends a confirmation message to the police personnel and logs the action.   
  
Alternative Flow:   
1. If the police personnel lacks the required permissions, the system displays an access denied message and logs the attempt.   
2. If the submitted form contains incomplete or invalid data, the system displays an error message and allows the user to correct the information.   
3. If the selected investigation or court case does not exist, the system prompts the user to enter a valid case ID.   
4. If the system encounters an error during record creation, it displays an error message and suggests retrying the action later.  
  
Use Case Name: Modify Criminal Information   
Use Case ID: UC-06   
Actors: Police Personnel, System, Administrator, Criminal Record   
  
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- A criminal record must already exist in the system and be associated with an investigation or court case.   
- The system is operational and accessible.   
  
Postconditions:   
- The criminal record is updated with the new information.   
- The system logs the modification for data integrity and audit purposes.   
- Notifications are sent to relevant stakeholders if the update affects the status of the case.   
- The system ensures access control is maintained throughout the process.   
  
Main Flow:   
1. The police personnel selects the "Modify Criminal Information" option from the case or record management menu.   
2. The system prompts the user to enter or select a criminal record ID.   
3. The system retrieves and displays the criminal record details.   
4. The police personnel edits the required information (e.g., name, offense details, sentence, or evidence).   
5. The police personnel submits the modified information.   
6. The system validates the input and updates the criminal record.   
7. The system links the modified record to the associated investigation or court case.   
8. The system logs the modification and sends a confirmation message to the police personnel.   
  
Alternative Flow:   
1. If the criminal record ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the police personnel lacks the required permissions to modify the criminal record, the system displays an access denied message and logs the attempt.   
3. If the submitted data is incomplete or invalid, the system displays an error message and allows the user to correct the input.   
4. If the system encounters an error during the modification process, it displays an error message and suggests retrying the action.   
5. If the modification triggers a significant status change in the associated case, the system notifies the administrator for review.  
  
Use Case Name: Delete Criminal Record   
Use Case ID: UC-07   
Actors: Police Personnel, System, Administrator   
  
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- A criminal record must exist in the system and be associated with an investigation or court case.   
- The system is operational and accessible.   
  
Postconditions:   
- The criminal record is successfully deleted from the system.   
- The system logs the deletion for data integrity and audit purposes.   
- The associated investigation or court case is updated to reflect the removal of the record.   
- The system ensures access control is maintained throughout the process.   
  
Main Flow:   
1. The police personnel selects the "Delete Criminal Record" option from the record management menu.   
2. The system prompts the user to enter or select a criminal record ID.   
3. The system retrieves and displays the criminal record details for confirmation.   
4. The police personnel confirms the deletion of the criminal record.   
5. The system validates the user's permissions and confirms the deletion request.   
6. The system deletes the criminal record from the database and updates the associated investigation or court case.   
7. The system logs the deletion and sends a confirmation message to the police personnel.   
  
Alternative Flow:   
1. If the criminal record ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the police personnel lacks the required permissions, the system displays an access denied message and logs the attempt.   
3. If the system encounters an error during deletion, it displays an error message and suggests retrying the action.   
4. If the deletion affects the status of the associated case, the system notifies the administrator for review.  
  
Use Case Name: View Court Case Details   
Use Case ID: UC-08   
Actors: Police Personnel, System, Citizen, Administrator, Court Case   
  
Preconditions:   
- The police personnel or citizen has access to the system and is logged in with appropriate permissions.   
- A court case must exist in the system and be associated with an investigation or complaint.   
- The system is operational and accessible.   
  
Postconditions:   
- The user can view detailed information about the court case.   
- The system ensures data integrity and access control during the viewing process.   
- If sensitive information is accessed, the system logs the activity for audit purposes.   
  
Main Flow:   
1. The police personnel or citizen selects the "View Court Case Details" option from the case dashboard or search menu.   
2. The system prompts the user to enter or select a court case ID.   
3. The system retrieves and displays all relevant details of the selected court case, including case status, associated complaint/investigation, involved parties, scheduled court dates, and any legal documents.   
4. The user reviews the information and may request additional details from the system.   
5. The system displays the requested information or prompts for clarification if the query is ambiguous.   
  
Alternative Flow:   
1. If the court case ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the user does not have permission to view the case, the system displays an access denied message and logs the unauthorized access attempt.   
3. If the system is unable to retrieve the case details due to a technical error, it displays an error message and suggests retrying the request.   
4. If the citizen requests to view the court case status, the system provides limited information based on the citizen's access rights and logs the access.  
  
Use Case Name: Update Court Case Status   
Use Case ID: UC-09   
Actors: Police Personnel, System, Administrator, Court Case   
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- A court case must exist in the system and be associated with an investigation or complaint.   
- The system is operational and accessible.   
  
Postconditions:   
- The court case status is updated in the system.   
- The update is linked to the associated investigation or complaint.   
- Notifications are sent to relevant stakeholders (e.g., police personnel, citizen, or administrator).   
- The system ensures data integrity and access control during the update process.   
  
Main Flow:   
1. The police personnel selects the "Update Court Case Status" option from the case management menu.   
2. The system displays the current court case status and provides a list of valid status options (e.g., "In Progress", "Closed", "On Hold", "Awaiting Trial").   
3. The police personnel selects a new status and optionally adds comments or attaches supporting documents.   
4. The police personnel submits the update request.   
5. The system validates the input and updates the court case status.   
6. The system links the update to the relevant investigation or complaint.   
7. The system sends a notification to the citizen and logs the update for audit purposes.   
  
Alternative Flow:   
1. If the selected status is invalid, the system displays an error message and prompts the user to choose a valid status.   
2. If the police personnel lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
3. If the court case ID is invalid or does not exist, the system prompts the user to enter a valid ID.   
4. If the system encounters an error while updating the court case, it displays an error message and suggests retrying the action.   
5. If the status change requires administrative approval, the system notifies the administrator for review before finalizing the update.  
  
Use Case Name: Manage Court Interaction   
Use Case ID: UC-10   
Actors: Police Personnel, System, Administrator, Court Case, Citizen   
Preconditions:   
- The police personnel or administrator has access to the system and is logged in with appropriate permissions.   
- A court case must exist and be linked to a registered complaint or investigation.   
- The system is operational and accessible.   
  
Postconditions:   
- The court case is updated or modified with new information or decisions.   
- All relevant parties (citizen, police, court) are notified of the changes.   
- The system maintains data integrity and access control.   
- The modification is logged for audit and compliance purposes.   
  
Main Flow:   
1. The police personnel or administrator selects the "Manage Court Interaction" option from the case management menu.   
2. The system displays the court case details along with the latest updates from the investigation or complaint.   
3. The user modifies the court case information, such as adding a court decision, updating the case timeline, or attaching legal documents.   
4. The user submits the changes.   
5. The system validates the input and updates the court case.   
6. The system links the update to the associated complaint or investigation.   
7. The system sends a notification to the citizen and relevant court case handler about the changes.   
8. The system logs the modification for audit and data integrity.   
  
Alternative Flow:   
1. If the user lacks the required permissions to modify the court case, the system displays an access denied message and logs the attempt.   
2. If the court case ID is invalid or does not exist, the system prompts the user to enter a valid ID.   
3. If the submitted data is incomplete or invalid, the system displays an error message and allows the user to correct the input.   
4. If the system encounters a technical error during the update, it displays an error message and suggests retrying the action.   
5. If the update triggers a need for administrative approval, the system notifies the administrator before applying the change.  
  
Use Case Name: View Citizen Information   
Use Case ID: UC-11   
Actors: Police Personnel, System, Administrator   
Preconditions:   
- The police personnel has access to the system and is logged in with appropriate permissions.   
- The citizen information must exist in the system.   
- The system is operational and accessible.   
  
Postconditions:   
- The police personnel can view the citizen's personal information and related case details.   
- The system ensures data integrity and access control during the viewing process.   
- The system logs the activity for audit purposes if sensitive information is accessed.   
  
Main Flow:   
1. The police personnel selects the "View Citizen Information" option from the case or citizen management menu.   
2. The system prompts the user to enter or select a citizen ID.   
3. The system retrieves and displays the citizen's personal information, including name, contact details, and any associated complaints or court cases.   
4. The police personnel reviews the information and may request additional details from the system.   
5. The system provides the requested information or prompts for clarification if the query is ambiguous.   
  
Alternative Flow:   
1. If the citizen ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the police personnel lacks the required permissions to view the information, the system displays an access denied message and logs the unauthorized access attempt.   
3. If the system is unable to retrieve the citizen's information due to a technical error, it displays an error message and suggests retrying the request.   
4. If the user requests access to sensitive data, the system verifies additional authorization and logs the access attempt.  
  
Use Case Name: Update Citizen Profile   
Use Case ID: UC-12   
Actors: Police Personnel, System, Administrator, Citizen   
  
Preconditions:   
- The police personnel or administrator has access to the system and is logged in with appropriate permissions.   
- The citizen profile must exist in the system and be associated with a registered account.   
- The system is operational and accessible.   
  
Postconditions:   
- The citizen profile is updated with the new or corrected information.   
- The system logs the modification for data integrity and audit purposes.   
- Notifications are sent to the citizen and relevant personnel if the update affects access or case details.   
- The system ensures access control is maintained during the update process.   
  
Main Flow:   
1. The police personnel or administrator selects the "Update Citizen Profile" option from the citizen management menu.   
2. The system prompts the user to enter or select a citizen ID.   
3. The system retrieves and displays the current citizen profile information.   
4. The user modifies the required fields (e.g., contact details, address, or personal information).   
5. The user submits the updated profile.   
6. The system validates the input data and confirms the submission.   
7. The system updates the citizen profile in the database.   
8. The system logs the update and sends a confirmation message to the user.   
  
Alternative Flow:   
1. If the citizen ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the user lacks the required permissions to modify the profile, the system displays an access denied message and logs the unauthorized attempt.   
3. If the submitted data is incomplete or invalid, the system displays an error message and allows the user to correct the input.   
4. If the system encounters an error during the update, it displays an error message and suggests retrying the action.   
5. If the citizen is notified of the update, the system ensures the notification complies with privacy policies and logs the activity.  
  
Use Case Name: Register Police Personnel   
Use Case ID: UC-13   
Actors: Administrator, System, Police Personnel   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The system is operational and accessible.   
- The police personnel has not yet been registered in the system.   
  
Postconditions:   
- The police personnel is successfully registered in the system.   
- A unique police personnel ID is assigned.   
- The system logs the registration for audit and data integrity.   
- The police personnel receives a confirmation message and login credentials (if applicable).   
  
Main Flow:   
1. The administrator selects the "Register Police Personnel" option from the user management menu.   
2. The system displays a registration form for police personnel, including fields for name, role, department, contact information, and authentication details.   
3. The administrator fills in the required information for the new police personnel.   
4. The administrator submits the registration form.   
5. The system validates the input data and confirms the submission.   
6. The system generates a unique police personnel ID and stores the information in the database.   
7. The system sends a confirmation message to the administrator and optionally to the police personnel.   
8. The system logs the registration for audit and data integrity purposes.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the submitted form contains incomplete or invalid data, the system displays an error message and allows the user to correct the input.   
3. If the system encounters an error while saving the registration, it displays an error message and suggests retrying the action.   
4. If the police personnel ID already exists in the system, the system displays a warning and prompts the administrator to check the input.  
  
Use Case Name: Assign Role to User   
Use Case ID: UC-14   
Actors: Administrator, System, Police Personnel, Citizen, Role   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The user (citizen or police personnel) must already exist in the system.   
- The system contains a predefined list of roles (e.g., "Police Officer", "Administrator", "Citizen").   
- The system is operational and accessible.   
  
Postconditions:   
- The user is assigned the specified role in the system.   
- The role assignment is recorded in the user profile and linked to the relevant configuration settings.   
- The system ensures access control is updated to reflect the new role.   
- The system logs the assignment for audit and data integrity.   
  
Main Flow:   
1. The administrator selects the "Assign Role to User" option from the user management menu.   
2. The system displays a list of registered users (e.g., citizen or police personnel) or allows the administrator to search for a specific user.   
3. The administrator selects the user to whom a role needs to be assigned.   
4. The system displays a list of available roles or allows the administrator to choose from predefined options.   
5. The administrator selects the appropriate role for the user.   
6. The administrator confirms the role assignment.   
7. The system validates the input and updates the user's profile with the new role.   
8. The system logs the assignment and updates access control policies accordingly.   
9. The system sends a confirmation message to the administrator indicating the successful role assignment.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the selected user does not exist in the system, the system displays an error message and prompts the administrator to enter a valid user ID.   
3. If the selected role is invalid or not supported, the system displays an error and prompts the administrator to choose a valid role.   
4. If the system encounters an error during role assignment, it displays an error message and suggests retrying the action.   
5. If the user is already assigned the selected role, the system displays a warning and prompts the administrator to choose a different role.  
  
Use Case Name: Modify Role Permissions   
Use Case ID: UC-15   
Actors: Administrator, System, Role, Police Personnel, Citizen   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- A role must exist in the system (e.g., "Police Officer", "Administrator", "Citizen").   
- The system is operational and accessible.   
  
Postconditions:   
- The role's permissions are updated in the system.   
- The system logs the modification for data integrity and audit purposes.   
- Access control policies are updated to reflect the new permissions.   
- The system ensures that only authorized users can modify role permissions.   
  
Main Flow:   
1. The administrator selects the "Modify Role Permissions" option from the role management menu.   
2. The system displays a list of available roles or allows the administrator to search for a specific role.   
3. The administrator selects the role whose permissions need to be modified.   
4. The system displays the current permissions assigned to the role.   
5. The administrator adjusts the permissions by enabling or disabling specific access rights (e.g., "Create Complaint", "Update Investigation", "View Criminal Records").   
6. The administrator confirms the changes.   
7. The system validates the input and updates the role's permissions in the configuration database.   
8. The system logs the modification and updates the access control policies accordingly.   
9. The system sends a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the selected role does not exist in the system, the system displays an error message and prompts the administrator to enter a valid role name.   
3. If the system detects an invalid permission configuration, it displays an error message and allows the administrator to correct the input.   
4. If the system encounters an error during the modification process, it displays an error message and suggests retrying the action.   
5. If the modification affects active users, the system may notify them of the updated role permissions or require a system restart to apply changes.  
  
Use Case Name: Configure System Settings   
Use Case ID: UC-16   
Actors: Administrator, System, Configuration, Security Feature, Access Control   
  
Preconditions:   
- The administrator has access to the system and is logged in with the appropriate permissions.   
- The system is operational and accessible.   
- A valid configuration or security feature exists in the system for modification or setup.   
  
Postconditions:   
- The system settings are updated according to the administrator's input.   
- The system logs the configuration change for audit and data integrity.   
- Access control policies are updated if necessary.   
- The system remains secure and functional after the configuration is applied.   
  
Main Flow:   
1. The administrator selects the "Configure System Settings" option from the system administration menu.   
2. The system displays a list of available settings categories (e.g., security settings, access control, user roles, notification preferences).   
3. The administrator selects a specific category to modify or configure.   
4. The system presents the current configuration values and allows the administrator to edit them.   
5. The administrator makes the necessary changes and submits the configuration.   
6. The system validates the input and applies the new settings.   
7. The system logs the configuration update and sends a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the attempt.   
2. If the selected configuration category does not exist, the system displays an error message and prompts the administrator to choose a valid option.   
3. If the system detects invalid or conflicting configuration settings, it displays an error message and allows the administrator to correct the input.   
4. If the system encounters an error while applying the configuration, it displays an error message and suggests retrying the action.   
5. If the configuration change affects existing user roles or access control policies, the system notifies relevant users or prompts the administrator to review the impact.  
  
Use Case Name: Update Configuration   
Use Case ID: UC-17   
Actors: Administrator, System, Configuration, Security Feature, Access Control   
  
Preconditions:   
- The administrator has access to the system and is logged in with the appropriate permissions.   
- The system is operational and accessible.   
- A configuration setting or security feature exists in the system for modification or setup.   
  
Postconditions:   
- The system configuration is updated according to the administrator's input.   
- The system logs the configuration change for audit and data integrity.   
- Access control policies are updated if the configuration change affects user permissions.   
- The system remains secure and functional after the update is applied.   
  
Main Flow:   
1. The administrator selects the "Update Configuration" option from the system settings menu.   
2. The system displays a list of configurable settings (e.g., system timeout, password policy, notification settings, or access control rules).   
3. The administrator selects the configuration to modify and enters the new values.   
4. The administrator submits the updated configuration.   
5. The system validates the input and confirms the configuration update.   
6. The system applies the new settings and updates the configuration database.   
7. The system logs the configuration change and sends a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the selected configuration does not exist, the system displays an error message and prompts the administrator to choose a valid configuration.   
3. If the system detects invalid or conflicting configuration values, it displays an error message and allows the administrator to correct the input.   
4. If the system encounters an error while applying the configuration, it displays an error message and suggests retrying the action.   
5. If the configuration change impacts access control policies, the system updates user permissions and may notify affected users of the change.  
  
Use Case Name: Manage Security Features   
Use Case ID: UC-18   
Actors: Administrator, System, Security Feature   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The system is operational and accessible.   
- At least one security feature exists in the system for modification or activation.   
  
Postconditions:   
- The security features in the system are updated or configured according to the administrator's input.   
- The system logs the security feature modification for audit and data integrity.   
- The system remains secure and functional after the changes are applied.   
  
Main Flow:   
1. The administrator selects the "Manage Security Features" option from the system administration menu.   
2. The system displays a list of available security features (e.g., two-factor authentication, role-based access control, encryption settings).   
3. The administrator selects a specific security feature to enable, disable, or modify.   
4. The system presents the current status and settings of the selected security feature.   
5. The administrator adjusts the feature settings or toggles its status (enabled/disabled).   
6. The administrator confirms the changes.   
7. The system validates the input and updates the security feature configuration.   
8. The system logs the change and sends a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the selected security feature does not exist, the system displays an error message and prompts the administrator to choose a valid feature.   
3. If the system detects invalid or conflicting security settings, it displays an error message and allows the administrator to correct the input.   
4. If the system encounters an error while applying the security feature changes, it displays an error message and suggests retrying the action.   
5. If the security feature update impacts access control or user permissions, the system may notify relevant users or require a system restart to apply changes.  
  
Use Case Name: Ensure Data Integrity   
Use Case ID: UC-19   
Actors: Administrator, System, Data Integrity, Access Control   
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The system is operational and accessible.   
- At least one data entity (e.g., complaint, criminal record, court case) exists in the system.   
  
Postconditions:   
- The system verifies and ensures the integrity of stored data.   
- Any inconsistencies or errors are flagged and reported to the administrator.   
- The system logs the data integrity check for audit purposes.   
- Access control policies are enforced during the integrity check process.   
  
Main Flow:   
1. The administrator selects the "Ensure Data Integrity" option from the system maintenance menu.   
2. The system initiates a data integrity check across all relevant data entities.   
3. The system verifies the consistency of data (e.g., complaint linked to an investigation, user roles aligned with access rights).   
4. The system identifies any discrepancies or corrupted data entries.   
5. The system generates a report summarizing the integrity status and any issues found.   
6. The system sends the report to the administrator for review and action.   
7. The system logs the integrity check process for audit and compliance.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the system encounters a technical error during the integrity check, it displays an error message and suggests retrying the action.   
3. If no data inconsistencies are found, the system sends a confirmation message to the administrator indicating all data is valid.   
4. If the system detects a critical integrity issue, it may suspend further operations until the administrator reviews the report and resolves the problem.  
  
Use Case Name: Control Access Rights   
Use Case ID: UC-20   
Actors: Administrator, System, Role, Police Personnel, Citizen   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The system is operational and accessible.   
- At least one user (citizen or police personnel) exists in the system.   
  
Postconditions:   
- The access rights of the user are updated according to the administrator's input.   
- The system logs the access control modification for audit and data integrity.   
- The user profile is updated with the new access rights.   
- The system enforces the updated access control policies immediately.   
  
Main Flow:   
1. The administrator selects the "Control Access Rights" option from the user management menu.   
2. The system displays a list of registered users or allows the administrator to search for a specific user.   
3. The administrator selects a user whose access rights need to be modified.   
4. The system displays the current access rights assigned to the selected user.   
5. The administrator adjusts the access rights by enabling or disabling specific permissions (e.g., "View Court Case", "Modify Complaint", "Delete Criminal Record").   
6. The administrator confirms the changes.   
7. The system validates the input and updates the user's access rights in the database.   
8. The system logs the access control modification and sends a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions, the system displays an access denied message and logs the unauthorized attempt.   
2. If the selected user does not exist in the system, the system displays an error message and prompts the administrator to enter a valid user ID.   
3. If the system detects invalid or conflicting access rights configuration, it displays an error message and allows the administrator to correct the input.   
4. If the system encounters an error during the access control update, it displays an error message and suggests retrying the action.   
5. If the user is already assigned the selected access rights, the system displays a warning and prompts the administrator to choose different rights.  
  
Use Case Name: View Access Logs   
Use Case ID: UC-21   
Actors: Administrator, System, Security Feature, Police Personnel   
  
Preconditions:   
- The administrator or authorized police personnel has access to the system and is logged in with appropriate permissions.   
- The system has access logs stored in the database.   
- The system is operational and accessible.   
  
Postconditions:   
- The access log details are displayed to the administrator or authorized personnel.   
- The system ensures data integrity and access control during the retrieval process.   
- The system logs the viewing activity for audit purposes.   
  
Main Flow:   
1. The administrator or authorized police personnel selects the "View Access Logs" option from the system administration menu.   
2. The system prompts the user to enter a search criteria (e.g., user ID, date range, or activity type).   
3. The system retrieves and displays the relevant access log entries, including timestamp, user, action performed, and affected data entity.   
4. The user reviews the access logs and may request additional filters or sorting options.   
5. The system applies the filters and displays the updated log entries.   
  
Alternative Flow:   
1. If the user lacks the required permissions to view access logs, the system displays an access denied message and logs the unauthorized attempt.   
2. If the system encounters an error while retrieving the access logs, it displays an error message and suggests retrying the action.   
3. If no matching access logs are found based on the search criteria, the system displays a message indicating no results were found.   
4. If the user provides invalid or unsupported filters, the system displays an error message and allows them to correct the input.  
  
Use Case Name: Track Case Progress   
Use Case ID: UC-22   
Actors: Police Personnel, System, Citizen, Administrator, Court Case   
  
Preconditions:   
- The police personnel or citizen has access to the system and is logged in with appropriate permissions.   
- An investigation or court case must exist in the system and be associated with a registered complaint.   
- The system is operational and accessible.   
  
Postconditions:   
- The user can view the current progress of the case, including status updates and timelines.   
- The system ensures data integrity and access control during the tracking process.   
- If sensitive information is accessed, the system logs the activity for audit purposes.   
  
Main Flow:   
1. The police personnel or citizen selects the "Track Case Progress" option from the case dashboard or search menu.   
2. The system prompts the user to enter or select a case ID (investigation or court case).   
3. The system retrieves and displays the current progress, including status, key events, assigned personnel, and related updates.   
4. The user reviews the progress and may request additional details or historical information.   
5. The system provides the requested information or prompts for clarification if the query is ambiguous.   
  
Alternative Flow:   
1. If the case ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the user does not have permission to view the case progress, the system displays an access denied message and logs the unauthorized access attempt.   
3. If the system is unable to retrieve the case details due to a technical error, it displays an error message and suggests retrying the request.   
4. If the user is a citizen and requests access to sensitive details, the system verifies access rights and provides only permitted information.  
  
Use Case Name: Manage Case Complaint Link   
Use Case ID: UC-23   
Actors: Police Personnel, System, Administrator   
  
Preconditions:   
- The police personnel or administrator has access to the system and is logged in with appropriate permissions.   
- An investigation case must exist in the system and be associated with a court case or complaint.   
- The system is operational and accessible.   
  
Postconditions:   
- The link between the case and the complaint is either created, modified, or removed based on the user's input.   
- The system logs the modification for data integrity and audit purposes.   
- Access control policies are enforced to ensure only authorized personnel can manage the link.   
- The associated complaint and case records are updated to reflect the new relationship.   
  
Main Flow:   
1. The police personnel or administrator selects the "Manage Case Complaint Link" option from the case or complaint management menu.   
2. The system prompts the user to enter or select a case ID (investigation or court case) and a complaint ID.   
3. The system retrieves and displays the current linking status between the selected case and complaint.   
4. The user chooses to either link the complaint to the case, modify an existing link (e.g., change the nature of the relationship), or remove the link.   
5. The user confirms the selected action.   
6. The system validates the input and updates the relationship between the case and complaint.   
7. The system logs the action for audit and data integrity purposes.   
8. The system sends a confirmation message to the user indicating the successful modification of the link.   
  
Alternative Flow:   
1. If the case ID or complaint ID is invalid or does not exist, the system displays an error message and prompts the user to enter valid IDs.   
2. If the user lacks the required permissions to manage the case-complaint link, the system displays an access denied message and logs the unauthorized attempt.   
3. If the system encounters an error during the linking or modification process, it displays an error message and suggests retrying the action.   
4. If the modification affects the status of the associated case or complaint, the system notifies the administrator for review.  
  
Use Case Name: View Police Personnel   
Use Case ID: UC-24   
Actors: Administrator, System, Police Personnel   
  
Preconditions:   
- The administrator or authorized police personnel has access to the system and is logged in with appropriate permissions.   
- The police personnel information must exist in the system.   
- The system is operational and accessible.   
  
Postconditions:   
- The user can view the personal and professional information of a police personnel.   
- The system ensures data integrity and access control during the viewing process.   
- If sensitive information is accessed, the system logs the activity for audit purposes.   
  
Main Flow:   
1. The administrator or authorized police personnel selects the "View Police Personnel" option from the user or personnel management menu.   
2. The system prompts the user to enter or select a police personnel ID.   
3. The system retrieves and displays the police personnel's information, including name, role, department, contact details, and any associated cases or assignments.   
4. The user reviews the information and may request additional details from the system.   
5. The system provides the requested information or prompts for clarification if the query is ambiguous.   
  
Alternative Flow:   
1. If the police personnel ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the user does not have permission to view the police personnel information, the system displays an access denied message and logs the unauthorized access attempt.   
3. If the system is unable to retrieve the police personnel's information due to a technical error, it displays an error message and suggests retrying the request.   
4. If the user requests access to highly sensitive data (e.g., disciplinary records), the system verifies additional authorization and logs the access attempt.  
  
Use Case Name: View Data Integrity   
Use Case ID: UC-25   
Actors: Administrator, System   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The system is operational and accessible.   
- Data integrity logs or reports must exist in the system for retrieval.   
  
Postconditions:   
- The administrator is able to view the data integrity status, including any flagged inconsistencies or errors.   
- The system ensures access control and data integrity during the retrieval and display process.   
- The viewing activity is logged for audit and compliance purposes.   
  
Main Flow:   
1. The administrator selects the "View Data Integrity" option from the system maintenance or audit menu.   
2. The system prompts the administrator to specify a time range, data entity type (e.g., complaint, criminal record, court case), or other filtering criteria.   
3. The system retrieves and displays the data integrity report, including details such as data validation results, inconsistencies, and timestamps of integrity checks.   
4. The administrator reviews the report and may request additional details for specific flagged entries.   
5. The system provides the requested details or prompts for clarification if the query is ambiguous.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions to view data integrity reports, the system displays an access denied message and logs the unauthorized attempt.   
2. If the system encounters an error while retrieving the data integrity report, it displays an error message and suggests retrying the action.   
3. If no integrity reports match the specified criteria, the system displays a message indicating no results were found.   
4. If the administrator requests access to highly sensitive integrity data, the system verifies additional authorization and logs the access attempt.  
  
Use Case Name: View Access Control   
Use Case ID: UC-26   
Actors: Administrator, System   
  
Preconditions:   
- The administrator has access to the system and is logged in with appropriate permissions.   
- The system contains access control configurations and user role definitions.   
- The system is operational and accessible.   
  
Postconditions:   
- The administrator can view the current access control policies and user permissions.   
- The system ensures data integrity and access control during the retrieval and display process.   
- The viewing activity is logged for audit and compliance purposes.   
  
Main Flow:   
1. The administrator selects the "View Access Control" option from the system administration or user management menu.   
2. The system displays a list of roles and their associated permissions, including details such as role name, assigned rights, and restrictions.   
3. The administrator can select a specific role to view its permissions in detail.   
4. The system retrieves and displays the role's access control configuration, including which data entities and actions are permitted.   
5. The administrator reviews the access control settings and may request additional filtering or sorting options.   
6. The system applies the filters and displays the updated access control information.   
7. The system logs the access control viewing activity for audit purposes.   
  
Alternative Flow:   
1. If the administrator lacks the required permissions to view access control settings, the system displays an access denied message and logs the unauthorized attempt.   
2. If the system encounters an error while retrieving access control information, it displays an error message and suggests retrying the action.   
3. If no access control configurations match the selected criteria, the system displays a message indicating no results were found.   
4. If the administrator requests access to highly sensitive access control data, the system verifies additional authorization and logs the access attempt.  
  
Use Case Name: Manage Court Case   
Use Case ID: UC-27   
Actors: Administrator, Police Personnel, System, Court Case   
  
Preconditions:   
- The administrator or police personnel has access to the system and is logged in with appropriate permissions.   
- A court case must exist in the system and be associated with a registered complaint or investigation.   
- The system is operational and accessible.   
  
Postconditions:   
- The court case is updated or modified with new or corrected information.   
- The system logs the modification for data integrity and audit purposes.   
- All relevant parties (e.g., citizen, police personnel, or court handler) are notified of the changes if required.   
- The system ensures access control is maintained and only authorized users can modify court case details.   
  
Main Flow:   
1. The administrator or police personnel selects the "Manage Court Case" option from the case management or court case handling menu.   
2. The system prompts the user to enter or select a court case ID.   
3. The system retrieves and displays the court case details, including the associated complaint or investigation, current status, involved parties, scheduled court dates, and any legal documents.   
4. The user modifies the court case information as needed (e.g., updates case status, adds legal documents, adjusts timelines, or modifies case details).   
5. The user submits the updated court case information.   
6. The system validates the input data and confirms the submission.   
7. The system updates the court case in the database and links it to the relevant complaint or investigation.   
8. The system sends notifications to relevant stakeholders (e.g., the citizen or court handler) if the update affects their interests.   
9. The system logs the modification and sends a confirmation message to the user.   
  
Alternative Flow:   
1. If the court case ID is invalid or does not exist, the system displays an error message and prompts the user to enter a valid ID.   
2. If the user lacks the required permissions to modify the court case, the system displays an access denied message and logs the unauthorized attempt.   
3. If the submitted data is incomplete or invalid, the system displays an error message and allows the user to correct the input.   
4. If the system encounters an error during the modification process, it displays an error message and suggests retrying the action.   
5. If the modification triggers a significant change in the case status, the system notifies the administrator for review.   
6. If the court case is linked to a complaint or investigation that requires additional verification, the system prompts the user to confirm the relationship before proceeding with the update.  
  
Use Case Name: Manage Citizen   
Use Case ID: UC-28   
Actors: Administrator, Police Personnel, System, Citizen   
  
Preconditions:   
- The administrator or police personnel has access to the system and is logged in with appropriate permissions.   
- The citizen information must exist in the system and be associated with a registered profile.   
- The system is operational and accessible.   
  
Postconditions:   
- The citizen's information is updated or modified in the system according to the administrator or police personnel's input.   
- The system logs the modification for data integrity and audit purposes.   
- The citizen profile remains secure and compliant with access control policies.   
- If the modification affects the citizen's access or case involvement, the system notifies the citizen and relevant personnel.   
  
Main Flow:   
1. The administrator or police personnel selects the "Manage Citizen" option from the user or citizen management menu.   
2. The system displays a list of registered citizens or allows the user to search for a specific citizen by ID or name.   
3. The user selects the citizen to be managed.   
4. The system retrieves and displays the citizen's profile, including personal information, contact details, and any associated complaints or court cases.   
5. The user modifies the required fields (e.g., contact details, personal information, or status).   
6. The user submits the updated information.   
7. The system validates the input data and confirms the submission.   
8. The system updates the citizen's profile in the database.   
9. The system logs the modification and sends a confirmation message to the administrator or police personnel.   
10. If necessary, the system notifies the citizen of the profile update.   
  
Alternative Flow:   
1. If the user lacks the required permissions to modify the citizen profile, the system displays an access denied message and logs the unauthorized attempt.   
2. If the selected citizen does not exist in the system, the system displays an error message and prompts the user to enter a valid citizen ID or name.   
3. If the submitted data is incomplete or invalid, the system displays an error message and allows the user to correct the input.   
4. If the system encounters an error during the update process, it displays an error message and suggests retrying the action.   
5. If the modification triggers a need for administrative approval (e.g., deactivating a citizen account), the system notifies the administrator for review before applying the change.