项目文档

# Functional Requirement

1.1 Complaint Registration Function   
Function ID: FR-01   
Description: Citizens can register a new complaint with the system. The system validates the input data, generates a unique complaint ID, and assigns the complaint to the appropriate criminal police personnel for investigation.   
Input: Complaint type, date, location, description of incident, and verified citizen identity.   
Output: A new complaint record stored in the system with a complaint ID and a confirmation message sent to the citizen.  
  
1.2 View Complaint Details Function   
Function ID: FR-02   
Description: Authorized actors (Security Administrator, Court Case Search, Criminal Police Personnel) can view the details of a registered complaint. The system logs the viewing action and displays any related court case information if available.   
Input: Valid complaint ID and actor credentials.   
Output: Complaint details displayed to the user, including type, date, location, description, and related court case information.  
  
1.3 Update Investigation Status Function   
Function ID: FR-03   
Description: Criminal Police Personnel or Security Administrators can update the status of an investigation. The system validates the update and logs the action. If the complaint is linked to a court case, the system updates the court case status accordingly.   
Input: Valid complaint ID, investigation status (e.g., "Under Investigation", "Solved", "Closed"), and optional notes or evidence.   
Output: Updated investigation status stored in the system, with status changes reflected in related court cases if applicable.  
  
1.4 Delete Investigation Record Function   
Function ID: FR-04   
Description: Security Administrators or Criminal Police Personnel can delete an existing investigation record. The system checks for authorization, logs the deletion, and updates the complaint and court case records if necessary.   
Input: Valid complaint ID and confirmation of deletion.   
Output: Investigation record removed from the database, and related records updated or unchanged as required.  
  
1.5 Register Criminal Information Function   
Function ID: FR-05   
Description: Criminal Police Personnel can register new criminal information based on a complaint. The system validates the data, generates a criminal information ID, and links the record to the complaint and court case, if applicable.   
Input: Valid complaint ID, suspect details, evidence, and witness statements.   
Output: A new criminal information record stored in the system, linked to the complaint and court case (if any).  
  
1.6 View Criminal Profile Function   
Function ID: FR-06   
Description: Authorized actors (Criminal Police Personnel, Security Administrator) can view the profile of a registered criminal. The system ensures data privacy and provides access to related complaints or court cases if linked.   
Input: Valid criminal ID or search criteria (e.g., name, crime type).   
Output: Criminal profile information displayed, including personal details, criminal history, and related case information.  
  
1.7 Modify Police Personnel Details Function   
Function ID: FR-07   
Description: Security Administrators or Criminal Police Personnel can modify the details of a registered police personnel. The system validates the updated data and logs the change.   
Input: Valid personnel ID and updated details (e.g., contact info, role, status).   
Output: Updated personnel record stored in the system, with access to the updated information for authorized users.  
  
1.8 Assign Case to Police Personnel Function   
Function ID: FR-08   
Description: Security Administrators can assign a case to a specific criminal police personnel. The system validates the personnel’s availability and role before assigning and logs the action.   
Input: Valid complaint or court case ID and valid personnel ID.   
Output: The case is assigned to the selected personnel, and the assignment is logged in the system.  
  
1.9 Remove Court Case Function   
Function ID: FR-09   
Description: Security Administrators or Criminal Police Personnel can remove a court case record. The system checks for active legal processes and logs the deletion.   
Input: Valid court case ID and confirmation of removal.   
Output: Court case record deleted from the database, with related complaint records updated if necessary.  
  
1.10 Update Court Case Information Function   
Function ID: FR-10   
Description: Security Administrators or Criminal Police Personnel can update the information of an existing court case. The system logs the action and updates the linked complaint or investigation records if applicable.   
Input: Valid court case ID and updated information (e.g., case status, judgment details).   
Output: Updated court case record stored in the system, with changes reflected in related complaint or investigation records.  
  
1.11 Search for Cases Function   
Function ID: FR-11   
Description: Authorized actors can search for cases using various criteria such as case ID, complaint ID, or crime type. The system retrieves and displays relevant results and logs the search action.   
Input: Search criteria (e.g., case ID, complaint ID, date range, crime type).   
Output: List of relevant case records displayed, including status, linked complaint, and court information.  
  
1.12 Search for Criminals Function   
Function ID: FR-12   
Description: Authorized actors can search for criminal records using identifiers such as name, criminal ID, or location. The system displays the results and logs the action.   
Input: Search criteria (e.g., name, criminal ID, crime type, location).   
Output: List of relevant criminal records displayed, including personal information, criminal history, and associated case details.  
  
1.13 Submit Feedback Function   
Function ID: FR-13   
Description: Citizens can submit feedback regarding a case or complaint. The system validates the input, generates a feedback ID, and logs the submission. If the feedback is linked to a case or court case, the system updates the status accordingly.   
Input: Feedback type, description, suggestions, and optional related complaint or court case ID.   
Output: A new feedback record stored in the system with a feedback ID and a confirmation message sent to the citizen.  
  
1.14 Citizen Views Case Updates Function   
Function ID: FR-14   
Description: Citizens can view the latest updates on their complaint or court case. The system checks for authorization, retrieves the case details, and logs the viewing action.   
Input: Valid complaint or court case ID and citizen credentials.   
Output: Latest case status, investigation progress, and related court case information displayed to the citizen.  
  
1.15 Assign Role to User Function   
Function ID: FR-15   
Description: Security Administrators can assign a role to a user account. The system validates the role and logs the assignment, ensuring that the user’s access level and functionality are updated.   
Input: Valid user ID and role ID or name.   
Output: Role assigned to the user, with updated access permissions and the action logged in the system.  
  
1.16 Modify System Configuration Function   
Function ID: FR-16   
Description: Security Administrators can modify system configurations such as access levels, notification settings, and role permissions. The system validates the configuration and logs the change.   
Input: Valid configuration parameters (e.g., access control rules, notification settings).   
Output: Updated system configuration stored in the database, with changes applied to user permissions and system behavior.  
  
1.17 Delete Configuration Function   
Function ID: FR-17   
Description: Security Administrators can delete a system configuration. The system checks for authorization, verifies the configuration's impact on roles, and logs the deletion.   
Input: Valid configuration ID and confirmation of deletion.   
Output: Configuration removed from the system, with associated role configurations updated if necessary.  
  
1.18 Enforce Security Policies Function   
Function ID: FR-18   
Description: Security Administrators can enforce or modify security policies. The system validates the policy, applies the changes, and logs the action.   
Input: Policy name, description, enforcement date, and role ID if applicable.   
Output: Updated or enforced security policies stored in the system, with changes reflected in the role configuration module.  
  
1.19 Manage Administrator Permissions Function   
Function ID: FR-19   
Description: Security Administrators can manage the permissions of other administrator accounts. The system validates the role configuration and logs the changes.   
Input: Valid administrator ID and updated role permissions.   
Output: Updated administrator permissions stored in the system, with the action logged for audit purposes.  
  
1.20 Manage Case Update Function   
Function ID: FR-20   
Description: Criminal Police Personnel or Security Administrators can manage case updates (create, edit, delete). The system validates the input, logs the action, and updates the court case search module if applicable.   
Input: Valid case or complaint ID, and update details (e.g., status, description, date).   
Output: Updated case record stored in the database, with the action logged and court case information updated if linked.  
  
1.21 Manage Feedback Record Function   
Function ID: FR-21   
Description: Security Administrators or Criminal Police Personnel can manage feedback records (view, update, resolve). The system logs the action and updates the related complaint or court case if necessary.   
Input: Valid feedback ID and action to be performed (e.g., update status, add resolution notes).   
Output: Feedback record updated in the database, with associated complaint or court case records updated and the citizen notified if applicable.  
  
1.22 Manage Assignment Log Function   
Function ID: FR-22   
Description: Security Administrators or Criminal Police Personnel can manage assignment logs (view, update, delete). The system logs the action and ensures that related records (case, complaint) are updated if necessary.   
Input: Valid assignment log ID or search criteria (e.g., case ID, personnel ID, date).   
Output: Assignment log updated or deleted, with the action logged and related records updated if applicable.  
  
1.23 Delete Complaint Function   
Function ID: FR-23   
Description: Security Administrators or Criminal Police Personnel can delete a complaint record. The system checks for active court cases and logs the deletion action.   
Input: Valid complaint ID and confirmation of deletion.   
Output: Complaint record removed from the database, with related court cases updated if necessary.  
  
1.24 Create Investigation Function   
Function ID: FR-24   
Description: Criminal Police Personnel or Security Administrators can create an investigation record for a complaint. The system validates the complaint and assigns the investigation to the appropriate personnel.   
Input: Valid complaint ID and details for the investigation (e.g., assigned personnel ID, initial status).   
Output: New investigation record stored in the database, with the complaint and court case (if any) updated accordingly.  
  
1.25 View Investigation Function   
Function ID: FR-25   
Description: Criminal Police Personnel or Security Administrators can view the details of an ongoing investigation. The system logs the action and displays related court case or complaint information if available.   
Input: Valid investigation ID and actor credentials.   
Output: Investigation details displayed, including complaint ID, personnel assigned, status, and any related court case information.  
  
1.26 Update Criminal Profile Function   
Function ID: FR-26   
Description: Criminal Police Personnel or Security Administrators can update a criminal’s profile. The system validates the input data and logs the update action.   
Input: Valid criminal ID and updated information (e.g., personal details, criminal history, investigation findings).   
Output: Updated criminal profile stored in the database, with related complaint or court case records updated if necessary.  
  
1.27 Delete Criminal Record Function   
Function ID: FR-27   
Description: Security Administrators or Criminal Police Personnel can delete a criminal record. The system checks for active court cases or investigations and logs the deletion.   
Input: Valid criminal ID and confirmation of deletion.   
Output: Criminal record removed from the database, with related records updated or invalidated if necessary.  
  
1.28 Create Police Personnel Function   
Function ID: FR-28   
Description: Security Administrators can create a new police personnel record. The system validates the input data, assigns a role, and logs the creation.   
Input: Personnel details (e.g., name, contact info, role, department) and valid role ID.   
Output: New police personnel record stored in the database with assigned role and the action logged.  
  
1.29 Delete Police Personnel Function   
Function ID: FR-29   
Description: Security Administrators can delete a police personnel record. The system checks for active assignments and logs the deletion action.   
Input: Valid personnel ID and confirmation of deletion.   
Output: Personnel record removed from the database, with related records updated or invalidated if necessary.  
  
1.30 Create Court Case Function   
Function ID: FR-30   
Description: Security Administrators or Criminal Police Personnel can create a new court case linked to an existing complaint or investigation. The system validates the input and logs the creation.   
Input: Valid complaint or investigation ID, and court case details (e.g., case type, filing date, legal status).   
Output: New court case record stored in the database and linked to the complaint and investigation.  
  
1.31 View Court Case Function   
Function ID: FR-31   
Description: Security Administrators or Criminal Police Personnel can view court case details. The system retrieves the data, logs the viewing action, and provides access to related complaint or investigation records if available.   
Input: Valid court case ID and actor credentials.   
Output: Court case details displayed, including type, filing date, legal status, and related complaint or investigation information.  
  
1.32 Delete Role Function   
Function ID: FR-32   
Description: Security Administrators can delete a role configuration. The system checks if the role is in use and logs the deletion action.   
Input: Valid role ID and confirmation of deletion.   
Output: Role record removed from the configuration database, with related user assignments invalidated if necessary.

# External Description

2. 外部接口（External Interfaces）   
  
本章描述系统与外部实体之间的接口，包括用户界面、硬件接口、软件接口和通信接口。这些接口定义了系统如何与用户、外部硬件、其他软件系统以及网络通信进行交互。   
  
---  
  
### 2.1 用户界面（User Interface）   
  
用户界面部分描述了系统与用户之间的交互方式，包括前端界面、数据输入方式、反馈显示机制等。   
  
- \*\*投诉登记界面\*\*：允许市民输入投诉类型、日期、地点、事件描述及验证身份信息，并显示生成的投诉编号和确认信息。   
- \*\*查看投诉详情界面\*\*：授权用户（安全管理员、法院案件查询人员、刑事警察人员）通过输入投诉编号和身份凭证查看投诉详情及关联的法院案件信息。   
- \*\*更新调查状态界面\*\*：刑事警察人员或安全管理员通过输入投诉编号和调查状态（如“调查中”、“已解决”、“已结案”）以及可选的备注或证据，更新调查状态。   
- \*\*删除调查记录界面\*\*：安全管理员或刑事警察人员通过输入投诉编号和删除确认信息，删除调查记录。   
- \*\*注册犯罪嫌疑人信息界面\*\*：刑事警察人员通过输入投诉编号、嫌疑人信息、证据和证人证词，注册新的犯罪嫌疑人记录。   
- \*\*查看犯罪嫌疑人信息界面\*\*：授权用户（安全管理员、刑事警察人员）通过输入犯罪嫌疑人编号或搜索条件，查看其个人资料、犯罪历史及关联案件。   
- \*\*修改警察人员信息界面\*\*：安全管理员或刑事警察人员通过输入人员编号及更新后的信息（如联系方式、角色、状态），修改警察人员记录。   
- \*\*分配案件给警察人员界面\*\*：安全管理员通过输入案件编号和警察人员编号，将案件分配给指定人员。   
- \*\*删除法院案件界面\*\*：安全管理员或刑事警察人员通过输入法院案件编号及删除确认信息，删除案件记录。   
- \*\*更新法院案件信息界面\*\*：安全管理员或刑事警察人员通过输入法院案件编号及更新后的信息（如案件状态、判决详情），更新案件记录。   
- \*\*案件搜索界面\*\*：授权用户通过输入案件编号、投诉编号、日期范围、犯罪类型等条件，搜索并查看相关案件信息。   
- \*\*犯罪嫌疑人搜索界面\*\*：授权用户通过输入姓名、犯罪嫌疑人编号、犯罪类型或地点，搜索并查看相关犯罪嫌疑人信息。   
- \*\*反馈提交界面\*\*：市民通过输入反馈类型、描述、建议及可选的投诉或法院案件编号，提交反馈。系统生成反馈编号并发送确认信息。   
- \*\*案件更新查看界面\*\*：市民通过输入投诉或法院案件编号及身份凭证，查看案件的最新状态、调查进度和相关法院案件信息。   
- \*\*角色分配界面\*\*：安全管理员通过输入用户编号及角色编号或名称，为用户分配角色，并记录系统日志。   
- \*\*系统配置管理界面\*\*：安全管理员通过输入配置参数（如访问控制规则、通知设置），修改系统配置。   
- \*\*安全策略管理界面\*\*：安全管理员通过输入安全策略名称、描述、生效日期及角色编号（如适用），执行或修改安全策略。   
- \*\*管理员权限管理界面\*\*：安全管理员通过输入管理员编号及更新后的角色权限，管理其他管理员的权限，并记录日志。   
- \*\*案件更新管理界面\*\*：刑事警察人员或安全管理员通过输入案件或投诉编号及更新细节（如状态、描述、日期），管理案件更新。   
- \*\*反馈记录管理界面\*\*：安全管理员或刑事警察人员通过输入反馈编号及操作（如更新状态、添加解决备注），管理反馈记录。   
- \*\*案件分配日志管理界面\*\*：安全管理员或刑事警察人员通过输入案件分配日志编号或搜索条件（如案件编号、人员编号、日期），管理分配日志记录。   
- \*\*投诉删除界面\*\*：安全管理员或刑事警察人员通过输入投诉编号及删除确认信息，删除投诉记录。   
- \*\*调查记录创建界面\*\*：刑事警察人员或安全管理员通过输入投诉编号及调查详情（如分配人员编号、初始状态），创建调查记录。   
- \*\*调查记录查看界面\*\*：刑事警察人员或安全管理员通过输入调查编号及身份凭证，查看调查详情及关联的法院案件或投诉信息。   
- \*\*犯罪嫌疑人资料更新界面\*\*：刑事警察人员或安全管理员通过输入犯罪嫌疑人编号及更新信息（如个人详情、犯罪记录、调查结果），更新犯罪嫌疑人资料。   
- \*\*犯罪嫌疑人记录删除界面\*\*：安全管理员或刑事警察人员通过输入犯罪嫌疑人编号及删除确认信息，删除记录。   
- \*\*警察人员记录创建界面\*\*：安全管理员通过输入人员详情（如姓名、联系方式、角色、部门）及有效角色编号，创建新的警察人员记录。   
- \*\*警察人员记录删除界面\*\*：安全管理员通过输入人员编号及删除确认信息，删除记录。   
- \*\*法院案件记录创建界面\*\*：安全管理员或刑事警察人员通过输入有效投诉或调查编号及法院案件详情（如案件类型、立案日期、法律状态），创建法院案件记录。   
- \*\*法院案件记录查看界面\*\*：安全管理员或刑事警察人员通过输入法院案件编号及身份凭证，查看案件详情及关联的投诉或调查记录。   
- \*\*角色删除界面\*\*：安全管理员通过输入角色编号及删除确认信息，删除角色配置。   
  
---  
  
### 2.2 硬件接口（Hardware Interface）   
  
本系统目前未涉及与外部硬件设备的直接交互，因此硬件接口部分为空。   
  
---  
  
### 2.3 软件接口（Software Interface）   
  
系统需要与多个内部数据库及可能的外部系统进行数据交互，具体软件接口如下：   
  
- \*\*投诉数据库（Complaint Database）\*\*   
 - \*\*接口描述\*\*：存储所有投诉记录，包括投诉编号、类型、日期、地点、事件描述、市民身份信息等。   
 - \*\*交互方式\*\*：系统通过SQL查询或NoSQL数据库接口读取和写入数据。   
 - \*\*输入\*\*：投诉信息（如投诉类型、时间、地点、描述等）。   
 - \*\*输出\*\*：投诉记录的创建、更新、删除或查询结果。   
  
- \*\*调查记录数据库（Investigation Database）\*\*   
 - \*\*接口描述\*\*：存储与投诉相关的调查记录，包括调查编号、状态、备注、证据、分配人员编号等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据的增删改查。   
 - \*\*输入\*\*：调查状态、备注、证据等。   
 - \*\*输出\*\*：调查记录的更新、删除或查询结果。   
  
- \*\*犯罪嫌疑人数据库（Criminal Database）\*\*   
 - \*\*接口描述\*\*：存储犯罪嫌疑人的个人信息、犯罪历史、相关案件编号等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据的读取和写入。   
 - \*\*输入\*\*：犯罪嫌疑人编号、姓名、犯罪类型、证据等。   
 - \*\*输出\*\*：犯罪嫌疑人记录的创建、更新、删除或查询结果。   
  
- \*\*法院案件数据库（Court Case Database）\*\*   
 - \*\*接口描述\*\*：存储法院案件的详细信息，包括案件编号、类型、立案日期、法律状态、判决详情等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据操作。   
 - \*\*输入\*\*：案件编号、案件类型、法律状态等。   
 - \*\*输出\*\*：法院案件记录的创建、更新、删除或查询结果。   
  
- \*\*人员管理数据库（Personnel Database）\*\*   
 - \*\*接口描述\*\*：存储警察人员的详细信息，包括人员编号、姓名、联系方式、角色、部门等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据操作。   
 - \*\*输入\*\*：人员编号、角色编号、更新信息等。   
 - \*\*输出\*\*：人员记录的创建、更新、删除或查询结果。   
  
- \*\*系统配置数据库（System Configuration Database）\*\*   
 - \*\*接口描述\*\*：存储系统的配置信息，包括访问控制规则、通知设置、角色权限等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据操作。   
 - \*\*输入\*\*：配置参数（如通知设置、访问控制规则）。   
 - \*\*输出\*\*：系统配置的更新或删除结果。   
  
- \*\*角色管理数据库（Role Management Database）\*\*   
 - \*\*接口描述\*\*：存储所有角色信息，包括角色编号、角色名称、权限列表等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据操作。   
 - \*\*输入\*\*：角色编号、角色名称、权限信息等。   
 - \*\*输出\*\*：角色信息的创建、更新、删除或查询结果。   
  
- \*\*反馈记录数据库（Feedback Database）\*\*   
 - \*\*接口描述\*\*：存储市民提交的反馈信息，包括反馈编号、反馈类型、描述、建议、关联案件编号等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据操作。   
 - \*\*输入\*\*：反馈类型、描述、建议、案件编号等。   
 - \*\*输出\*\*：反馈记录的创建、更新、删除或查询结果。   
  
- \*\*案件分配日志数据库（Assignment Log Database）\*\*   
 - \*\*接口描述\*\*：记录案件分配的历史信息，包括分配编号、案件编号、人员编号、分配时间等。   
 - \*\*交互方式\*\*：通过数据库接口进行数据操作。   
 - \*\*输入\*\*：案件编号、人员编号、分配时间等。   
 - \*\*输出\*\*：案件分配记录的创建、更新、删除或查询结果。   
  
---  
  
### 2.4 通信接口（Communication Interface）   
  
本系统通过以下方式与外部进行通信：   
  
- \*\*电子邮件通知（Email Notification）\*\*   
 - \*\*接口描述\*\*：系统通过SMTP协议向市民发送确认信息、案件更新通知及反馈提交确认。   
 - \*\*交互方式\*\*：使用标准邮件API进行消息发送。   
 - \*\*输入\*\*：发送对象（市民邮箱）、通知内容（如案件状态、投诉编号、反馈编号等）。   
 - \*\*输出\*\*：邮件发送成功或失败的状态信息。   
  
- \*\*短信通知（SMS Notification）\*\*   
 - \*\*接口描述\*\*：系统通过短信API向市民或相关人员发送案件状态变更、反馈提交等通知。   
 - \*\*交互方式\*\*：使用第三方短信平台提供的API接口。   
 - \*\*输入\*\*：接收号码、通知内容。   
 - \*\*输出\*\*：短信发送状态及日志记录。   
  
- \*\*系统日志接口（System Log Interface）\*\*   
 - \*\*接口描述\*\*：系统通过日志记录模块记录所有用户操作，包括案件查看、状态更新、记录删除等。   
 - \*\*交互方式\*\*：使用本地日志文件或日志数据库接口。   
 - \*\*输入\*\*：操作类型（如“查看”、“更新”、“删除”）、操作时间、操作用户、相关记录编号。   
 - \*\*输出\*\*：日志记录的写入结果。   
  
- \*\*用户身份验证接口（User Authentication Interface）\*\*   
 - \*\*接口描述\*\*：系统通过身份验证模块验证用户（市民、警察人员、管理员）的权限。   
 - \*\*交互方式\*\*：通过内部认证数据库或集成的外部认证服务（如LDAP、OAuth）进行验证。   
 - \*\*输入\*\*：用户凭证（如用户名和密码）、角色权限检查请求。   
 - \*\*输出\*\*：认证结果（成功/失败）及用户角色权限信息。   
  
- \*\*案件状态同步接口（Case Status Synchronization Interface）\*\*   
 - \*\*接口描述\*\*：系统在更新调查状态或法院案件状态时，同步更新相关联的数据库记录。   
 - \*\*交互方式\*\*：通过数据库触发器或系统内部状态同步模块实现。   
 - \*\*输入\*\*：案件编号、状态更新信息。   
 - \*\*输出\*\*：关联记录（如投诉、法院案件）的状态更新结果。   
  
- \*\*案件通知推送接口（Case Update Push Notification Interface）\*\*   
 - \*\*接口描述\*\*：系统向市民推送案件的最新状态或调查进展。   
 - \*\*交互方式\*\*：通过WebSocket、Push API或第三方消息推送服务（如Firebase Cloud Messaging）实现。   
 - \*\*输入\*\*：接收用户ID、案件编号、更新信息。   
 - \*\*输出\*\*：通知消息发送成功或失败的状态。   
  
---  
  
### 2.5 与其他系统的接口（Interface with External Systems）   
  
- \*\*法院案件查询系统（Court Case Search System）\*\*   
 - \*\*接口描述\*\*：系统与法院案件查询模块交互，提供案件关联信息。   
 - \*\*交互方式\*\*：通过内部API调用或数据库关联查询。   
 - \*\*输入\*\*：案件编号、查询条件。   
 - \*\*输出\*\*：案件详细信息（如判决状态、法律依据等）。   
  
- \*\*用户权限管理模块（User Role and Permission Module）\*\*   
 - \*\*接口描述\*\*：系统与用户权限管理模块交互，实现用户角色分配、权限修改及删除。   
 - \*\*交互方式\*\*：通过内部API调用或数据库操作。   
 - \*\*输入\*\*：用户ID、角色ID、权限配置信息。   
 - \*\*输出\*\*：角色分配、权限更新或删除结果。   
  
- \*\*安全策略管理模块（Security Policy Management Module）\*\*   
 - \*\*接口描述\*\*：系统与安全策略管理模块交互，执行或更新安全策略。   
 - \*\*交互方式\*\*：通过内部API调用或数据库操作。   
 - \*\*输入\*\*：安全策略名称、描述、生效日期、关联角色ID。   
 - \*\*输出\*\*：策略执行结果或更新状态。   
  
---  
  
### 2.6 数据导入/导出接口（Data Import/Export Interface）   
  
- \*\*数据导出接口\*\*   
 - \*\*接口描述\*\*：系统支持将案件、投诉、人员等数据导出为CSV、Excel或PDF格式，供审计或分析使用。   
 - \*\*交互方式\*\*：通过文件导出API或用户界面操作。   
 - \*\*输入\*\*：导出类型（案件、投诉、人员）、导出格式、筛选条件。   
 - \*\*输出\*\*：导出的文件及下载链接。   
  
- \*\*数据导入接口\*\*   
 - \*\*接口描述\*\*：系统支持通过上传文件方式导入案件、人员或配置数据。   
 - \*\*交互方式\*\*：通过文件导入API或用户界面操作。   
 - \*\*输入\*\*：导入文件（CSV、Excel）、字段映射配置。   
 - \*\*输出\*\*：导入结果（成功/失败）及日志记录。   
  
---  
  
### 2.7 外部API接口（External API Interface）   
  
- \*\*短信服务API（SMS Service API）\*\*   
 - \*\*接口描述\*\*：系统通过第三方短信服务API发送案件或反馈相关的通知。   
 - \*\*交互方式\*\*：RESTful API调用。   
 - \*\*输入\*\*：短信内容、接收号码。   
 - \*\*输出\*\*：API响应状态（成功/失败）、发送时间戳。   
  
- \*\*邮件服务API（Email Service API）\*\*   
 - \*\*接口描述\*\*：系统通过邮件服务API发送确认信息、案件更新通知等。   
 - \*\*交互方式\*\*：RESTful API或SMTP协议。   
 - \*\*输入\*\*：邮件内容、发送地址、接收地址。   
 - \*\*输出\*\*：邮件发送状态及日志。   
  
---  
  
本章详细描述了系统与外部实体的交互方式，包括用户界面、数据库、通信接口及其他系统模块。所有外部数据源均已在上述接口中定义并分类，确保系统功能的正确实现和数据的一致性。

# Use Case

Use Case Name: Complaint Registration   
Use Case ID: UC-01   
Actors: Citizen, Security Administrator, Court Case Search   
Preconditions:   
1. The citizen has access to the complaint registration system.   
2. The citizen has a valid identity verified by the system.   
3. The system is operational and connected to the police and court databases.   
  
Postconditions:   
1. A new complaint has been successfully recorded in the system.   
2. The complaint is assigned to the appropriate criminal police personnel for investigation.   
3. The citizen receives a confirmation message with a complaint ID for future reference.   
  
Main Flow:   
1. The citizen logs in to the complaint registration system.   
2. The citizen selects the type of complaint (e.g., theft, assault, fraud).   
3. The citizen fills out the complaint form with relevant details (e.g., date, location, description of incident).   
4. The system validates the form data for completeness and accuracy.   
5. The system generates a unique complaint ID and stores the complaint in the database.   
6. The system sends a confirmation message to the citizen with the complaint ID.   
7. The system assigns the complaint to the relevant criminal police personnel for investigation.   
  
Alternative Flow:   
1. If the form data is incomplete or inaccurate, the system displays an error message and prompts the citizen to correct the information.   
2. If the system fails to generate a complaint ID, the security administrator is notified for manual intervention.   
3. If the complaint is related to an existing court case, the court case search module is triggered to verify and link the complaint to the appropriate case.  
  
Use Case Name: View Complaint Details   
Use Case ID: UC-02   
Actors: Security Administrator, Court Case Search, Criminal Police Personnel   
Preconditions:   
1. The complaint has been registered in the system with a valid complaint ID.   
2. The actor (Security Administrator, Court Case Search, or Criminal Police Personnel) has access to the complaint viewing system.   
3. The actor has been authenticated and authorized to view complaint details.   
  
Postconditions:   
1. The complaint details are displayed to the authorized actor.   
2. The viewing action is logged in the system for audit purposes.   
3. If the complaint is linked to an existing court case, the court case details are also accessible.   
  
Main Flow:   
1. The actor logs in to the complaint management system.   
2. The actor navigates to the complaint details section.   
3. The actor enters or selects a valid complaint ID.   
4. The system retrieves the complaint details from the database.   
5. The system displays the complaint details to the actor, including type, date, location, and incident description.   
6. If the complaint is linked to a court case, the system shows the related court case information.   
  
Alternative Flow:   
1. If the complaint ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to view the complaint, the system denies access and logs the unauthorized attempt.   
3. If the system is unable to retrieve the complaint due to database issues, the system alerts the security administrator for resolution.  
  
Use Case Name: Update Investigation Status   
Use Case ID: UC-03   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
Preconditions:   
1. The complaint has been registered in the system with a valid complaint ID.   
2. The criminal police personnel have been assigned to investigate the complaint.   
3. The actor (Criminal Police Personnel or Security Administrator) has access to the investigation status update system.   
4. The system is connected to the court case search module if needed.   
  
Postconditions:   
1. The investigation status for the complaint is updated in the system.   
2. The updated status is visible to authorized personnel and the security administrator.   
3. If the complaint is linked to a court case, the court case status is also updated accordingly.   
4. The update action is logged in the system for audit purposes.   
  
Main Flow:   
1. The criminal police personnel log in to the complaint management system.   
2. The personnel navigate to the assigned complaint using the complaint ID.   
3. The system displays the current investigation status and relevant details.   
4. The personnel select or modify the investigation status (e.g., "Under Investigation", "Solved", "Closed").   
5. The personnel provide additional notes or evidence as needed.   
6. The system updates the investigation status in the database.   
7. The system notifies the security administrator of the update if required.   
8. If the complaint is linked to a court case, the system updates the court case status through the court case search module.   
  
Alternative Flow:   
1. If the complaint ID is invalid or not found, the system displays an error message and prompts the personnel to enter a valid ID.   
2. If the personnel do not have authorization to update the status, the system denies access and logs the unauthorized attempt.   
3. If the system fails to update the database, the security administrator is alerted for manual correction.   
4. If the court case status update fails, the system logs the error and provides a warning to the personnel.  
  
Use Case Name: Delete Investigation Record   
Use Case ID: UC-04   
Actors: Security Administrator, Criminal Police Personnel   
Preconditions:   
1. The complaint has been registered and an investigation record has been created.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the investigation record deletion system.   
3. The actor has been authenticated and authorized to perform deletion operations.   
4. The complaint ID is valid and corresponds to an existing investigation record.   
  
Postconditions:   
1. The investigation record is removed from the system.   
2. The deletion is logged for audit and traceability purposes.   
3. If the investigation record is linked to a court case, the court case status is updated to reflect the deletion.   
4. The associated complaint remains in the system unless explicitly deleted through another use case.   
  
Main Flow:   
1. The actor logs in to the complaint management system.   
2. The actor navigates to the investigation record section.   
3. The actor enters or selects a valid complaint ID.   
4. The system retrieves and displays the investigation record for confirmation.   
5. The actor confirms the deletion of the record.   
6. The system deletes the investigation record from the database.   
7. The system logs the deletion action and updates the complaint status if necessary.   
8. If applicable, the system updates the linked court case status via the court case search module.   
9. The system displays a confirmation message indicating the successful deletion.   
  
Alternative Flow:   
1. If the complaint ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to delete the investigation record, the system denies access and logs the unauthorized attempt.   
3. If the system fails to delete the record due to database constraints or errors, it alerts the security administrator for manual resolution.   
4. If the actor cancels the deletion during the confirmation step, the system returns to the previous screen without making any changes.   
5. If the deletion of the record affects a linked court case and the court case status update fails, the system logs the error and notifies the actor.  
  
Use Case Name: Register Criminal Information   
Use Case ID: UC-05   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
Preconditions:   
1. The criminal police personnel have access to the criminal information registration system.   
2. The personnel are authenticated and authorized to register criminal information.   
3. The system is connected to the court case search module to verify existing cases.   
4. A valid complaint has already been registered in the system.   
  
Postconditions:   
1. A new criminal information record has been successfully created and stored in the system.   
2. The criminal information is linked to the corresponding complaint and court case if applicable.   
3. The registration action is logged for audit purposes.   
4. The security administrator is notified if the registration triggers specific alerts or rules.   
  
Main Flow:   
1. The criminal police personnel log in to the system.   
2. The personnel navigate to the criminal information registration section.   
3. The system displays the list of registered complaints for selection.   
4. The personnel select a complaint by entering or choosing a valid complaint ID.   
5. The system retrieves the complaint details and displays them for reference.   
6. The personnel input criminal-related information (e.g., suspect details, evidence, witness statements).   
7. The system validates the input data for accuracy and relevance.   
8. The system generates a unique criminal information ID and stores the data in the database.   
9. The system logs the registration action and notifies the security administrator if needed.   
10. If the complaint is linked to a court case, the system updates the court case with the new criminal information.   
  
Alternative Flow:   
1. If the complaint ID is invalid or not found, the system displays an error message and prompts the personnel to enter a valid ID.   
2. If the personnel do not have authorization to register criminal information, the system denies access and logs the unauthorized attempt.   
3. If the system fails to validate the criminal information data, it prompts the user to correct the input.   
4. If the system fails to generate a criminal information ID, the security administrator is alerted for manual intervention.   
5. If the court case update fails, the system logs the error and notifies the personnel for follow-up.  
  
Use Case Name: View Criminal Profile   
Use Case ID: UC-06   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
Preconditions:   
1. A criminal profile has been registered in the system.   
2. The actor has access to the criminal profile viewing system.   
3. The actor has been authenticated and authorized to view criminal profiles.   
4. The system is connected to the court case search module if needed.   
  
Postconditions:   
1. The criminal profile details are displayed to the authorized actor.   
2. The viewing action is logged in the system for audit purposes.   
3. If the criminal is linked to a court case, the related court case information is also accessible.   
  
Main Flow:   
1. The actor logs in to the criminal management system.   
2. The actor navigates to the criminal profile section.   
3. The actor enters or selects a valid criminal ID or searches by name/other identifiers.   
4. The system retrieves the criminal profile from the database.   
5. The system displays the criminal profile, including personal information, criminal history, and any associated complaints or court cases.   
6. If the criminal is linked to a court case, the system provides access to the court case details via the court case search module.   
  
Alternative Flow:   
1. If the criminal ID or search criteria are invalid or not found, the system displays an error message and prompts the actor to provide valid input.   
2. If the actor does not have authorization to view the criminal profile, the system denies access and logs the unauthorized attempt.   
3. If the system is unable to retrieve the criminal profile due to database issues, it alerts the security administrator for resolution.   
4. If the criminal is linked to a court case and the system fails to retrieve it, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Modify Police Personnel Details   
Use Case ID: UC-07   
Actors: Security Administrator, Criminal Police Personnel   
Preconditions:   
1. The police personnel details are already stored in the system.   
2. The actor (Security Administrator or Criminal Police Personnel with appropriate permissions) has access to the police personnel modification system.   
3. The system is operational and connected to the personnel database.   
4. The personnel ID is valid and corresponds to an existing police personnel record.   
  
Postconditions:   
1. The police personnel details are updated in the system.   
2. The modification action is logged for audit purposes.   
3. The updated details are accessible to authorized personnel.   
  
Main Flow:   
1. The actor logs in to the police personnel management system.   
2. The actor navigates to the personnel modification section.   
3. The actor enters or selects a valid personnel ID.   
4. The system retrieves and displays the current personnel details.   
5. The actor modifies the required information (e.g., contact details, role, status).   
6. The system validates the modified data for accuracy and compliance.   
7. The system updates the personnel record in the database.   
8. The system logs the modification action.   
9. The system displays a confirmation message indicating the successful modification.   
  
Alternative Flow:   
1. If the personnel ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to modify police personnel details, the system denies access and logs the unauthorized attempt.   
3. If the system fails to validate the modified data, it displays an error and prompts the actor to correct the input.   
4. If the system fails to update the personnel record due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the actor cancels the modification during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Assign Case to Police Personnel   
Use Case ID: UC-08   
Actors: Security Administrator, Court Case Search, Criminal Police Personnel   
Preconditions:   
1. A valid complaint or court case has been registered in the system.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the case assignment system.   
3. The actor is authenticated and authorized to assign cases.   
4. The police personnel database contains available personnel with valid IDs.   
  
Postconditions:   
1. The complaint or court case is assigned to a specific criminal police personnel.   
2. The assignment is logged in the system for audit and tracking purposes.   
3. The assigned personnel receive a notification about the case.   
4. If the case is linked to a court case, the assignment is reflected in the court case record.   
  
Main Flow:   
1. The actor logs in to the complaint or court case management system.   
2. The actor navigates to the case assignment section.   
3. The actor selects a complaint or court case by entering a valid complaint/case ID.   
4. The system retrieves the complaint or court case details.   
5. The actor searches for and selects a suitable criminal police personnel by entering or choosing a valid personnel ID.   
6. The system validates the personnel's availability and role.   
7. The system assigns the case to the selected police personnel and updates the database.   
8. The system logs the assignment action.   
9. The system sends a notification to the assigned police personnel about the new case.   
10. If the case is linked to a court case, the system updates the court case record to reflect the assignment.   
  
Alternative Flow:   
1. If the complaint or court case ID is invalid, the system displays an error and prompts for a valid ID.   
2. If the police personnel ID is invalid or the personnel is not available, the system shows an error and requests a valid selection.   
3. If the actor is not authorized to assign cases, the system denies access and logs the attempt.   
4. If the system fails to update the assignment in the database, it alerts the security administrator for manual correction.   
5. If the notification to the police personnel fails, the system logs the error and allows the actor to retry or notify manually.   
6. If the court case update fails, the system logs the error and prompts the actor for follow-up action.  
  
Use Case Name: Remove Court Case   
Use Case ID: UC-09   
Actors: Security Administrator, Criminal Police Personnel   
Preconditions:   
1. A court case has been registered in the system with a valid case ID.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the court case removal system.   
3. The actor is authenticated and authorized to perform removal operations.   
4. The court case is not currently in a critical legal process (e.g., active trial, pending judgment).   
  
Postconditions:   
1. The court case is removed from the system.   
2. The removal action is logged for audit and traceability purposes.   
3. If the court case was linked to a complaint, the complaint status is updated to reflect the removal.   
4. The system ensures data integrity and does not delete associated complaint records unless explicitly handled by other use cases.   
  
Main Flow:   
1. The actor logs in to the court case management system.   
2. The actor navigates to the court case removal section.   
3. The actor enters or selects a valid court case ID.   
4. The system retrieves and displays the court case details for confirmation.   
5. The actor confirms the removal of the court case.   
6. The system deletes the court case record from the database.   
7. The system updates the status of the linked complaint (if any) to reflect the removal.   
8. The system logs the removal action.   
9. The system displays a confirmation message indicating the successful removal.   
  
Alternative Flow:   
1. If the court case ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to remove the court case, the system denies access and logs the unauthorized attempt.   
3. If the court case is linked to an active legal process, the system displays a warning and prevents removal until the status is updated.   
4. If the system fails to delete the court case due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the actor cancels the removal during the confirmation step, the system returns to the previous screen without making any changes.   
6. If the system fails to update the complaint status after removal, it logs the error and notifies the actor for follow-up.  
  
Use Case Name: Update Court Case Information   
Use Case ID: UC-10   
Actors: Security Administrator, Criminal Police Personnel, Court Case Search   
Preconditions:   
1. A court case has been registered in the system with a valid case ID.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the court case update system.   
3. The actor is authenticated and authorized to update court case information.   
4. The system is connected to the court case search module to verify the case details.   
  
Postconditions:   
1. The court case information is updated in the system.   
2. The update is logged for audit and traceability purposes.   
3. If the court case is linked to a complaint, the complaint record is updated accordingly.   
4. The updated information is visible to authorized personnel.   
  
Main Flow:   
1. The actor logs in to the court case management system.   
2. The actor navigates to the court case update section.   
3. The actor enters or selects a valid court case ID.   
4. The system retrieves and displays the current court case details.   
5. The actor modifies the required information (e.g., case status, judgment details, court schedule).   
6. The system validates the updated data for accuracy and compliance.   
7. The system updates the court case record in the database.   
8. The system logs the update action.   
9. If the court case is linked to a complaint, the system updates the complaint record accordingly.   
10. The system displays a confirmation message indicating the successful update.   
  
Alternative Flow:   
1. If the court case ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to update the court case, the system denies access and logs the unauthorized attempt.   
3. If the system fails to validate the updated data, it displays an error and prompts the actor to correct the input.   
4. If the system fails to update the court case due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the actor cancels the update during the confirmation step, the system returns to the previous screen without making any changes.   
6. If the system fails to update the linked complaint record, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Search for Cases   
Use Case ID: UC-11   
Actors: Security Administrator, Criminal Police Personnel, Court Case Search   
Preconditions:   
1. The actor has access to the case search system.   
2. The actor is authenticated and authorized to perform case searches.   
3. The system is connected to the police and court databases.   
4. There are existing records in the system for complaints or court cases.   
  
Postconditions:   
1. The actor receives a list of relevant cases based on the search criteria.   
2. The search action is logged in the system for audit purposes.   
3. If the case is linked to a complaint or criminal profile, the related information is accessible.   
  
Main Flow:   
1. The actor logs in to the case search system.   
2. The actor navigates to the case search section.   
3. The actor enters search criteria (e.g., case ID, complaint ID, date range, type of crime).   
4. The system queries the relevant databases for matching records.   
5. The system displays the search results, including case details (e.g., status, linked complaint, court information).   
6. The actor selects a specific case for detailed viewing or further action.   
  
Alternative Flow:   
1. If no records match the search criteria, the system displays a message indicating no results.   
2. If the actor enters invalid or incomplete search criteria, the system prompts for correction.   
3. If the system fails to retrieve the search results due to database issues, it alerts the security administrator for resolution.   
4. If the actor does not have authorization to view certain case details, the system restricts access and logs the attempt.  
  
Use Case Name: Search for Criminals   
Use Case ID: UC-12   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
Preconditions:   
1. The system contains records of registered criminals with valid criminal IDs.   
2. The actor (Criminal Police Personnel or Security Administrator) has access to the criminal search system.   
3. The actor is authenticated and authorized to perform criminal searches.   
4. The system is connected to the court case search module if required for case linkage.   
  
Postconditions:   
1. The actor receives a list of matching criminal records based on the search criteria.   
2. The search action is logged in the system for audit and traceability purposes.   
3. If a criminal is linked to a court case, the case details are accessible through the court case search module.   
  
Main Flow:   
1. The actor logs in to the criminal management system.   
2. The actor navigates to the criminal search section.   
3. The actor enters search criteria (e.g., name, criminal ID, crime type, or location).   
4. The system queries the criminal database for matching records.   
5. The system displays the search results, including criminal details (e.g., name, personal information, crime history, and linked complaints or court cases).   
6. The actor selects a specific criminal for detailed viewing or further investigation.   
  
Alternative Flow:   
1. If no records match the search criteria, the system displays a message indicating no results found.   
2. If the search criteria are invalid or incomplete, the system prompts the actor to correct the input.   
3. If the system fails to retrieve data due to database issues, it alerts the security administrator for resolution.   
4. If the actor does not have authorization to view certain criminal details, the system restricts access and logs the unauthorized attempt.   
5. If the system fails to link a criminal to a court case, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Submit Feedback   
Use Case ID: UC-13   
Actors: Citizen, Security Administrator, Court Case Search   
Preconditions:   
1. The citizen has access to the feedback submission system.   
2. The citizen has a valid identity verified by the system.   
3. The system is operational and connected to the police and court databases if necessary.   
4. The citizen may or may not have a related complaint or court case to reference.   
  
Postconditions:   
1. A new feedback record is successfully stored in the system.   
2. The feedback is associated with a complaint or court case, if applicable.   
3. The citizen receives a confirmation message with a feedback ID for future reference.   
4. The feedback is accessible to the security administrator for review and action.   
  
Main Flow:   
1. The citizen logs in to the feedback submission system.   
2. The citizen selects the type of feedback (e.g., system usability, police response time, court procedures).   
3. The citizen fills out the feedback form with relevant details (e.g., description, suggestions, related complaint/case ID).   
4. The system validates the form data for completeness and accuracy.   
5. The system generates a unique feedback ID and stores the feedback in the database.   
6. The system sends a confirmation message to the citizen with the feedback ID.   
7. The system logs the submission and notifies the security administrator if a complaint or court case is referenced.   
8. If the feedback is related to an existing court case, the court case search module is used to verify and link the feedback.   
  
Alternative Flow:   
1. If the form data is incomplete or inaccurate, the system displays an error message and prompts the citizen to correct the information.   
2. If the system fails to generate a feedback ID, the security administrator is notified for manual intervention.   
3. If the referenced complaint or court case ID is invalid, the system displays an error and allows the citizen to remove or correct the reference.   
4. If the citizen does not reference a complaint or court case, the feedback is still submitted and stored as a standalone record.   
5. If the system fails to notify the security administrator, an error is logged and the citizen is informed that their feedback has been recorded but manual follow-up may be required.  
  
Use Case Name: Citizen Views Case Updates   
Use Case ID: UC-14   
Actors: Citizen, Court Case Search, Security Administrator   
Preconditions:   
1. The citizen has a valid complaint or court case ID to reference.   
2. The citizen is authenticated and authorized to view updates related to the case.   
3. The system is connected to the police and court case databases.   
4. The complaint or court case is in an active or updated status.   
  
Postconditions:   
1. The citizen receives the latest updates on the case.   
2. The viewing action is logged in the system for audit purposes.   
3. If the case is linked to a court case, the system displays the related court case status and details.   
4. The system ensures data privacy and only displays information the citizen is authorized to view.   
  
Main Flow:   
1. The citizen logs in to the case tracking system.   
2. The citizen navigates to the case update viewing section.   
3. The citizen enters or selects a valid complaint or court case ID.   
4. The system retrieves the case and its latest updates from the database.   
5. The system displays the case status, investigation progress, and any related court case information if applicable.   
6. The system logs the viewing action in the audit trail.   
7. The citizen is informed if no recent updates are available.   
  
Alternative Flow:   
1. If the case ID is invalid or not found, the system displays an error message and prompts the citizen to enter a valid ID.   
2. If the citizen does not have authorization to view the case, the system denies access and logs the unauthorized attempt.   
3. If the system fails to retrieve case updates due to database issues, it alerts the security administrator for resolution.   
4. If the case is linked to a court case and the court case information cannot be retrieved, the system logs the error and informs the citizen of the issue.  
  
Use Case Name: Assign Role to User   
Use Case ID: UC-15   
Actors: Security Administrator, Role Configuration   
Preconditions:   
1. The user account exists in the system.   
2. The actor (Security Administrator) has access to the role assignment system.   
3. The actor is authenticated and authorized to assign roles.   
4. The role configuration module contains valid roles.   
  
Postconditions:   
1. The user is assigned a valid role in the system.   
2. The role assignment is logged in the system for audit purposes.   
3. The assigned role determines the user's access level and functionality.   
4. If the role is linked to specific modules (e.g., Court Case Search), the user can access those modules accordingly.   
  
Main Flow:   
1. The security administrator logs in to the user management system.   
2. The administrator navigates to the role assignment section.   
3. The administrator selects a user account by entering or choosing a valid user ID.   
4. The system retrieves and displays the user’s current role (if any).   
5. The administrator selects a new role from the role configuration module.   
6. The system validates the selected role for compatibility with the user account.   
7. The system updates the user’s role in the database.   
8. The system logs the role assignment action.   
9. The system displays a confirmation message indicating the successful assignment.   
  
Alternative Flow:   
1. If the user ID is invalid or not found, the system displays an error and prompts the administrator to enter a valid ID.   
2. If the selected role is invalid or not available, the system displays an error and requests a valid role selection.   
3. If the administrator is not authorized to assign roles, the system denies access and logs the unauthorized attempt.   
4. If the system fails to update the role in the database, it alerts the security administrator for manual correction.   
5. If the role assignment affects access to other modules (e.g., Court Case Search) and the update fails, the system logs the error and notifies the administrator for follow-up.  
  
Use Case Name: Modify System Configuration   
Use Case ID: UC-16   
Actors: Security Administrator, Role Configuration   
Preconditions:   
1. The system configuration is stored in the database.   
2. The actor (Security Administrator) has access to the system configuration modification interface.   
3. The actor is authenticated and authorized to modify system settings.   
4. The role configuration module contains valid role definitions for reference.   
  
Postconditions:   
1. The system configuration is updated according to the specified changes.   
2. The modification action is logged for audit and traceability.   
3. The updated configuration affects user permissions or system behavior based on the role definitions.   
4. The system remains operational after the configuration is applied.   
  
Main Flow:   
1. The security administrator logs in to the system configuration management module.   
2. The administrator navigates to the system configuration editing section.   
3. The system displays the current configuration settings.   
4. The administrator selects or modifies configuration parameters (e.g., access levels, notification settings, system roles).   
5. The system validates the modified configuration for consistency and role compatibility.   
6. The system updates the configuration in the database.   
7. The system logs the modification action with the administrator's details.   
8. The system confirms the configuration update and applies the changes.   
  
Alternative Flow:   
1. If the configuration parameters are invalid or conflicting, the system displays an error and prompts for correction.   
2. If the system fails to validate the configuration, the administrator is notified and the update is not applied.   
3. If the administrator does not have the required authorization, the system denies access and logs the attempt.   
4. If the system fails to update the configuration in the database, an error is logged and the administrator is alerted for manual resolution.   
5. If the modification affects role-based access and the update fails, the system logs the error and notifies the administrator for follow-up.  
  
Use Case Name: Delete Configuration   
Use Case ID: UC-17   
Actors: Security Administrator, Role Configuration   
Preconditions:   
1. The system configuration is stored in the database.   
2. The actor (Security Administrator) has access to the configuration deletion interface.   
3. The actor is authenticated and authorized to delete system configurations.   
4. The configuration to be deleted is identified by a valid configuration ID.   
  
Postconditions:   
1. The specified configuration is removed from the system.   
2. The deletion action is logged in the system for audit and traceability purposes.   
3. If the configuration was linked to specific user roles, the role configuration module is updated accordingly.   
4. The system remains functional after the deletion.   
  
Main Flow:   
1. The security administrator logs in to the configuration management system.   
2. The administrator navigates to the configuration deletion section.   
3. The administrator enters or selects a valid configuration ID.   
4. The system retrieves and displays the configuration details for confirmation.   
5. The administrator confirms the deletion of the configuration.   
6. The system deletes the configuration from the database.   
7. The system updates the role configuration module if necessary.   
8. The system logs the deletion action.   
9. The system displays a confirmation message indicating the successful deletion.   
  
Alternative Flow:   
1. If the configuration ID is invalid or not found, the system displays an error message and prompts the administrator to enter a valid ID.   
2. If the administrator does not have authorization to delete the configuration, the system denies access and logs the unauthorized attempt.   
3. If the system fails to delete the configuration due to database constraints or errors, it alerts the security administrator for manual resolution.   
4. If the configuration is linked to active user roles and the update to the role configuration fails, an error is logged, and the administrator is notified for follow-up.   
5. If the administrator cancels the deletion during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Enforce Security Policies   
Use Case ID: UC-18   
Actors: Security Administrator, Role Configuration, Criminal Police Personnel   
Preconditions:   
1. The system contains defined security policies and access control rules.   
2. The actor (Security Administrator) has access to the security policy enforcement system.   
3. The actor is authenticated and authorized to enforce or modify security policies.   
4. The role configuration module is connected and operational.   
  
Postconditions:   
1. The security policies are enforced or modified in the system.   
2. The enforcement or modification action is logged for audit and traceability purposes.   
3. The role configuration module is updated to reflect any changes in access control.   
4. The system remains secure and functional after the policy enforcement.   
  
Main Flow:   
1. The security administrator logs in to the system security management module.   
2. The administrator navigates to the security policy enforcement section.   
3. The system displays the current active security policies and access control rules.   
4. The administrator selects a specific policy to enforce or modify (e.g., access permissions, data encryption rules).   
5. The administrator updates the policy settings or applies new policies.   
6. The system validates the updated policy for consistency with role definitions and system integrity.   
7. The system enforces the new or updated policy and updates the relevant modules (e.g., Role Configuration).   
8. The system logs the enforcement action with the administrator’s details.   
9. The system displays a confirmation message indicating the successful enforcement of the policy.   
  
Alternative Flow:   
1. If the selected policy is invalid or not supported, the system displays an error message and prompts the administrator to select a valid policy.   
2. If the system fails to validate the updated policy, the administrator is notified and the enforcement is not applied.   
3. If the administrator does not have the required authorization, the system denies access and logs the unauthorized attempt.   
4. If the system fails to enforce the policy due to database or configuration errors, an error is logged, and the administrator is alerted for manual resolution.   
5. If the policy update affects role-based access and the role configuration fails to update, the system logs the error and notifies the administrator for follow-up.   
6. If the administrator cancels the enforcement during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Manage Administrator Permissions   
Use Case ID: UC-19   
Actors: Security Administrator, Role Configuration   
Preconditions:   
1. The system has a valid role configuration module with defined administrator roles.   
2. The actor (Security Administrator) has access to the administrator permissions management system.   
3. The actor is authenticated and authorized to modify administrator permissions.   
4. The administrator account to be managed exists in the system.   
  
Postconditions:   
1. The administrator's permissions are updated or managed based on the role configuration.   
2. The modification is logged in the system for audit and traceability purposes.   
3. The updated permissions take effect immediately for the administrator account.   
4. The role configuration is synchronized with the system to maintain access control consistency.   
  
Main Flow:   
1. The security administrator logs in to the system and navigates to the administrator permissions management interface.   
2. The administrator selects an administrator account by entering or choosing a valid user ID.   
3. The system retrieves and displays the current permissions assigned to the selected administrator.   
4. The administrator modifies the permissions by selecting or unselecting roles from the role configuration module.   
5. The system validates the selected roles for compatibility and availability.   
6. The system updates the administrator's permissions in the database.   
7. The system logs the modification action with the administrator's details.   
8. The system displays a confirmation message indicating the successful update.   
  
Alternative Flow:   
1. If the user ID is invalid or not found, the system displays an error message and prompts the administrator to enter a valid ID.   
2. If the selected roles are not valid or not available, the system displays an error and requests a valid role selection.   
3. If the administrator is not authorized to modify permissions, the system denies access and logs the unauthorized attempt.   
4. If the system fails to validate the role configuration, the administrator is notified, and the modification is not applied.   
5. If the system fails to update the administrator's permissions in the database, an error is logged, and the security administrator is alerted for manual resolution.   
6. If the administrator cancels the modification during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Manage Case Update   
Use Case ID: UC-20   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
  
Preconditions:   
1. A court case or complaint has been registered in the system with a valid case or complaint ID.   
2. The actor (Criminal Police Personnel or Security Administrator) has access to the case update management system.   
3. The actor is authenticated and authorized to manage updates for the case.   
4. The system is connected to the court case search module to verify and retrieve case details.   
  
Postconditions:   
1. The case update is managed, including creation, modification, or deletion of update records.   
2. The update action is logged in the system for audit and traceability purposes.   
3. If the case is linked to a court case, the court case search module is updated to reflect the changes.   
4. The system ensures that only authorized actors can perform update management actions.   
  
Main Flow:   
1. The actor logs in to the case update management system.   
2. The actor navigates to the case update management section.   
3. The actor selects a case by entering a valid case or complaint ID.   
4. The system retrieves the case details and displays the current list of updates.   
5. The actor selects an action to manage the updates (e.g., add new update, edit existing update, delete update).   
6. If adding a new update, the actor provides the update details (e.g., status, description, date, related evidence).   
7. If editing or deleting an update, the actor selects the specific update record to modify or remove.   
8. The system validates the update data for accuracy and compliance with case management rules.   
9. The system performs the selected action (create, update, or delete) and modifies the case update record in the database.   
10. The system logs the update management action and notifies the security administrator if needed.   
11. If the case is linked to a court case, the system updates the court case search module with the new information.   
12. The system displays a confirmation message indicating the successful management of the case update.   
  
Alternative Flow:   
1. If the case or complaint ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to manage case updates, the system denies access and logs the unauthorized attempt.   
3. If the system fails to validate the update data, it displays an error and prompts the actor to correct the input.   
4. If the system fails to perform the selected management action due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the actor cancels the management action during the confirmation step, the system returns to the previous screen without making any changes.   
6. If the update is linked to a court case and the court case search module fails to update, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Manage Feedback Record   
Use Case ID: UC-21   
Actors: Security Administrator, Criminal Police Personnel, Court Case Search   
  
Preconditions:   
1. A feedback record has been submitted to the system with a valid feedback ID.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the feedback record management system.   
3. The actor is authenticated and authorized to manage feedback records.   
4. The system is connected to the court case search module if the feedback is linked to a court case.   
  
Postconditions:   
1. The feedback record is managed (e.g., viewed, updated, or resolved) in the system.   
2. The management action is logged for audit and traceability purposes.   
3. If the feedback is linked to a court case or complaint, the associated record is updated or referenced accordingly.   
4. The citizen who submitted the feedback is notified of any resolution or response, if applicable.   
  
Main Flow:   
1. The actor logs in to the feedback management system.   
2. The actor navigates to the feedback record management section.   
3. The actor enters or selects a valid feedback ID to manage the record.   
4. The system retrieves and displays the feedback details, including the type of feedback, description, related complaint/case ID (if any), and current status.   
5. The actor selects an action to perform on the feedback (e.g., view details, update status, add a resolution note).   
6. If updating the feedback status, the actor selects a new status (e.g., "Under Review", "Resolved", "Pending").   
7. The actor provides additional comments or resolution details if necessary.   
8. The system validates the input for accuracy and applies the selected action.   
9. If the feedback is linked to a court case or complaint, the system updates the associated record with the new status or notes.   
10. The system logs the management action in the audit trail.   
11. If applicable, the system sends a notification to the citizen who submitted the feedback.   
12. The system displays a confirmation message indicating the successful management of the feedback record.   
  
Alternative Flow:   
1. If the feedback ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to manage the feedback record, the system denies access and logs the unauthorized attempt.   
3. If the system fails to retrieve the feedback record, it alerts the security administrator for resolution.   
4. If the system fails to validate the input (e.g., invalid status selection), it displays an error and prompts the actor to correct the input.   
5. If the update affects a linked court case or complaint and the system fails to update the associated record, an error is logged, and the actor is notified for follow-up.   
6. If the notification to the citizen fails, the system logs the error and allows the actor to manually inform the citizen.   
7. If the actor cancels the management action during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Manage Assignment Log   
Use Case ID: UC-22   
Actors: Security Administrator, Criminal Police Personnel, Court Case Search   
  
Preconditions:   
1. An assignment log record exists in the system, documenting the assignment of a case to a specific police personnel.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the assignment log management system.   
3. The actor is authenticated and authorized to view, update, or delete assignment logs.   
4. The system is connected to the case and personnel databases to retrieve related information.   
  
Postconditions:   
1. The assignment log is successfully managed (e.g., viewed, updated, or deleted).   
2. The management action is logged in the system for audit and traceability purposes.   
3. If the assignment log is linked to a court case or complaint, the system ensures the relevant information remains consistent.   
4. The system remains secure and functional after the log is managed.   
  
Main Flow:   
1. The actor logs in to the assignment log management system.   
2. The actor navigates to the assignment log section.   
3. The actor enters or selects a valid assignment log ID or searches for a log using related criteria (e.g., case ID, personnel ID, date range).   
4. The system retrieves and displays the relevant assignment log entries.   
5. The actor selects a specific assignment log for management (e.g., view, update, delete).   
6. If viewing, the system displays the full details of the log, including the case ID, personnel ID, assignment date, and status.   
7. If updating, the actor modifies the log details (e.g., reassigning the case to another personnel, updating the assignment status).   
8. If deleting, the system confirms the deletion and removes the log from the database.   
9. The system validates all changes for accuracy and compliance with system rules.   
10. The system updates the assignment log in the database based on the selected action.   
11. The system logs the management action in the audit trail.   
12. If the assignment log is linked to a court case or complaint, the system updates the relevant record to reflect any changes.   
13. The system displays a confirmation message indicating the successful management of the assignment log.   
  
Alternative Flow:   
1. If the assignment log ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to manage the assignment log, the system denies access and logs the unauthorized attempt.   
3. If the system fails to retrieve the assignment log due to database issues, it alerts the security administrator for resolution.   
4. If the system fails to validate the input data (e.g., incorrect personnel ID or invalid case ID), it displays an error and prompts the actor to correct the input.   
5. If the system fails to update or delete the assignment log due to database constraints or errors, it alerts the security administrator for manual resolution.   
6. If the update or deletion of the assignment log affects a linked court case or complaint and the system fails to update the associated record, an error is logged, and the actor is notified for follow-up.   
7. If the actor cancels the management action during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Delete Complaint   
Use Case ID: UC-23   
Actors: Security Administrator, Criminal Police Personnel   
  
Preconditions:   
1. The complaint has been registered in the system with a valid complaint ID.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the complaint deletion system.   
3. The actor is authenticated and authorized to perform complaint deletion operations.   
4. The complaint is not currently linked to an active court case or critical legal process.   
  
Postconditions:   
1. The complaint is removed from the system.   
2. The deletion is logged in the system for audit and traceability purposes.   
3. If the complaint was linked to a court case, the system checks and updates the court case status accordingly.   
4. The system ensures data integrity and does not delete associated criminal or court records unless explicitly handled by other use cases.   
  
Main Flow:   
1. The actor logs in to the complaint management system.   
2. The actor navigates to the complaint deletion section.   
3. The actor enters or selects a valid complaint ID.   
4. The system retrieves and displays the complaint details for confirmation.   
5. The system verifies whether the complaint is linked to an active court case.   
6. If no active court case is linked, the actor confirms the deletion of the complaint.   
7. The system deletes the complaint record from the database.   
8. The system logs the deletion action with the actor's details.   
9. If the complaint was linked to a court case, the system updates the court case record to remove the link.   
10. The system displays a confirmation message indicating the successful deletion.   
  
Alternative Flow:   
1. If the complaint ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to delete the complaint, the system denies access and logs the unauthorized attempt.   
3. If the complaint is linked to an active court case, the system displays a warning and prevents deletion until the court case status is reviewed and updated.   
4. If the system fails to delete the complaint due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the actor cancels the deletion during the confirmation step, the system returns to the previous screen without making any changes.   
6. If the system fails to update the court case record after removing the link, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Create Investigation   
Use Case ID: UC-24   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
  
Preconditions:   
1. A valid complaint has been registered in the system with a complaint ID.   
2. The actor (Criminal Police Personnel or Security Administrator) has access to the investigation creation system.   
3. The actor is authenticated and authorized to create an investigation.   
4. The system is connected to the court case search module for potential case linkage.   
  
Postconditions:   
1. A new investigation record is created in the system and linked to the complaint.   
2. The investigation record is assigned to the responsible criminal police personnel.   
3. The creation action is logged for audit and traceability purposes.   
4. If the complaint is linked to a court case, the court case record is updated to reflect the new investigation.   
  
Main Flow:   
1. The criminal police personnel or security administrator logs in to the investigation management system.   
2. The actor navigates to the investigation creation section.   
3. The actor enters or selects a valid complaint ID to initiate an investigation.   
4. The system retrieves the complaint details and confirms that it is eligible for investigation.   
5. The actor selects or assigns the criminal police personnel responsible for the investigation.   
6. The system validates the personnel's availability and role for the assignment.   
7. The system creates a new investigation record, including the complaint ID, assigned personnel ID, and initial investigation status.   
8. The system stores the investigation record in the database.   
9. The system logs the investigation creation action.   
10. If the complaint is linked to a court case, the system updates the court case record to reflect the new investigation.   
11. The system displays a confirmation message indicating the successful creation of the investigation.   
  
Alternative Flow:   
1. If the complaint ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the complaint is already under investigation, the system displays a warning and prevents duplicate investigation creation.   
3. If the assigned personnel ID is invalid or the personnel is not available, the system displays an error and requests a valid personnel selection.   
4. If the system fails to create the investigation record due to database issues, it alerts the security administrator for resolution.   
5. If the actor is not authorized to create an investigation, the system denies access and logs the unauthorized attempt.   
6. If the court case update fails after linking the investigation, the system logs the error and notifies the actor for follow-up.   
7. If the actor cancels the investigation creation during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: View Investigation   
Use Case ID: UC-25   
Actors: Criminal Police Personnel, Security Administrator, Court Case Search   
  
Preconditions:   
1. The investigation record has been created in the system with a valid investigation ID.   
2. The actor (Criminal Police Personnel or Security Administrator) has access to the investigation viewing system.   
3. The actor is authenticated and authorized to view investigation details.   
4. The system is connected to the court case search module if the investigation is linked to a court case.   
  
Postconditions:   
1. The investigation details are displayed to the authorized actor.   
2. The viewing action is logged in the system for audit and traceability purposes.   
3. If the investigation is linked to a court case, the court case details are accessible through the court case search module.   
4. The system ensures data privacy and only displays information the actor is authorized to view.   
  
Main Flow:   
1. The actor logs in to the investigation management system.   
2. The actor navigates to the investigation viewing section.   
3. The actor enters or selects a valid investigation ID.   
4. The system retrieves the investigation details from the database.   
5. The system displays the investigation details, including the complaint ID, assigned personnel, investigation status, and notes.   
6. If the investigation is linked to a court case, the system shows the related court case information via the court case search module.   
7. The system logs the viewing action in the audit trail.   
  
Alternative Flow:   
1. If the investigation ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to view the investigation, the system denies access and logs the unauthorized attempt.   
3. If the system fails to retrieve the investigation due to database issues, it alerts the security administrator for resolution.   
4. If the court case linkage is present and the system fails to retrieve the court case details, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Update Criminal Profile   
Use Case ID: UC-26   
Actors: Criminal Police Personnel, Security Administrator   
  
Preconditions:   
1. A criminal profile has been registered in the system with a valid criminal ID.   
2. The actor (Criminal Police Personnel or Security Administrator) has access to the criminal profile update system.   
3. The actor is authenticated and authorized to update criminal profiles.   
4. The system is connected to the criminal profile database and any linked court case or complaint records.   
  
Postconditions:   
1. The criminal profile is updated in the system with the new or modified information.   
2. The update action is logged in the system for audit and traceability purposes.   
3. If the criminal profile is linked to a court case or complaint, the related records are updated accordingly.   
4. The system ensures data integrity and privacy during the update process.   
  
Main Flow:   
1. The actor logs in to the criminal profile management system.   
2. The actor navigates to the criminal profile update section.   
3. The actor enters or selects a valid criminal ID.   
4. The system retrieves the current criminal profile and displays it for editing.   
5. The actor modifies the required information (e.g., personal details, criminal history, recent investigation findings).   
6. The system validates the modified data for accuracy and compliance with data rules.   
7. The system updates the criminal profile in the database.   
8. The system logs the update action, including the actor's details and the changes made.   
9. If the criminal profile is linked to a court case or complaint, the system updates the related records to reflect the changes.   
10. The system displays a confirmation message indicating the successful update of the criminal profile.   
  
Alternative Flow:   
1. If the criminal ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to update the criminal profile, the system denies access and logs the unauthorized attempt.   
3. If the system fails to validate the updated data (e.g., inconsistent or incomplete criminal history), it displays an error and prompts the actor to correct the information.   
4. If the system fails to update the criminal profile due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the update affects a linked court case or complaint and the system fails to update those records, an error is logged and the actor is notified for follow-up.   
6. If the actor cancels the update during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Delete Criminal Record   
Use Case ID: UC-27   
Actors: Security Administrator, Criminal Police Personnel   
  
Preconditions:   
1. A criminal record has been registered in the system with a valid criminal ID.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the criminal record deletion system.   
3. The actor is authenticated and authorized to perform criminal record deletion operations.   
4. The criminal record is not currently linked to an active court case or under active investigation.   
  
Postconditions:   
1. The criminal record is removed from the system.   
2. The deletion action is logged in the system for audit and traceability purposes.   
3. If the criminal record was linked to a court case or complaint, the system checks and updates the relevant records to remove the link.   
4. The system ensures data integrity and does not delete associated investigation or feedback records unless explicitly handled by other use cases.   
  
Main Flow:   
1. The actor logs in to the criminal management system.   
2. The actor navigates to the criminal record deletion section.   
3. The actor enters or selects a valid criminal ID.   
4. The system retrieves and displays the criminal record details for confirmation.   
5. The system verifies whether the criminal is linked to any active court cases or complaints.   
6. If no active links exist, the actor confirms the deletion of the criminal record.   
7. The system deletes the criminal record from the database.   
8. The system logs the deletion action with the actor's details.   
9. If the criminal record was linked to a court case or complaint, the system updates the associated records to remove the reference.   
10. The system displays a confirmation message indicating the successful deletion of the criminal record.   
  
Alternative Flow:   
1. If the criminal ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to delete the criminal record, the system denies access and logs the unauthorized attempt.   
3. If the criminal record is linked to an active court case or complaint, the system displays a warning and prevents deletion until the links are resolved or updated.   
4. If the system fails to delete the criminal record due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the actor cancels the deletion during the confirmation step, the system returns to the previous screen without making any changes.   
6. If the system fails to update the linked court case or complaint records after deletion, an error is logged, and the actor is notified for follow-up.  
  
Use Case Name: Create Police Personnel   
Use Case ID: UC-28   
Actors: Security Administrator, Role Configuration   
  
Preconditions:   
1. The security administrator has access to the police personnel creation system.   
2. The administrator is authenticated and authorized to create new police personnel records.   
3. The system is connected to the personnel database and the role configuration module.   
4. A valid role (e.g., Criminal Police Personnel) exists in the role configuration for assignment.   
  
Postconditions:   
1. A new police personnel record is successfully created and stored in the system.   
2. The personnel is assigned a valid role based on the role configuration.   
3. The creation action is logged in the system for audit and traceability purposes.   
4. The new police personnel can now be assigned to cases or manage investigations, depending on their role.   
  
Main Flow:   
1. The security administrator logs in to the police personnel management system.   
2. The administrator navigates to the police personnel creation section.   
3. The administrator enters the necessary details for the new police personnel (e.g., name, contact information, role, department, status).   
4. The system validates the input data for completeness and role compatibility.   
5. The system generates a unique personnel ID and stores the new police personnel record in the database.   
6. The system assigns the selected role to the personnel using the role configuration module.   
7. The system logs the creation action, including the administrator's details and the personnel's information.   
8. The system displays a confirmation message indicating the successful creation of the police personnel record.   
  
Alternative Flow:   
1. If the input data is incomplete or invalid, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected role is not valid or not available in the role configuration, the system displays an error and requests a valid role selection.   
3. If the system fails to generate a personnel ID, the security administrator is alerted for manual intervention.   
4. If the system fails to assign the role due to configuration issues, it logs the error and notifies the administrator for follow-up.   
5. If the system fails to store the personnel record in the database, it alerts the security administrator for manual resolution.   
6. If the administrator cancels the creation during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Delete Police Personnel   
Use Case ID: UC-29   
Actors: Security Administrator   
  
Preconditions:   
1. A police personnel record has been created in the system with a valid personnel ID.   
2. The actor (Security Administrator) has access to the police personnel deletion system.   
3. The actor is authenticated and authorized to perform deletion operations on police personnel records.   
4. The police personnel is not currently assigned to any active complaint or court case.   
5. The system is connected to the personnel database and the role configuration module.   
  
Postconditions:   
1. The police personnel record is removed from the system.   
2. The deletion action is logged for audit and traceability purposes.   
3. If the personnel was previously assigned a role, the role configuration module is updated to reflect the change.   
4. Any references to the personnel in other system modules (e.g., assignment logs, case records) are either removed or marked as invalid, ensuring data integrity.   
5. The system remains operational and secure after the deletion.   
  
Main Flow:   
1. The security administrator logs in to the police personnel management system.   
2. The administrator navigates to the personnel deletion section.   
3. The administrator enters or selects a valid personnel ID.   
4. The system retrieves and displays the personnel details for confirmation.   
5. The system checks if the personnel is currently assigned to any active complaint or court case.   
6. If no active assignments are found, the administrator confirms the deletion.   
7. The system deletes the police personnel record from the database.   
8. The system updates the role configuration module to remove the personnel from any assigned roles.   
9. The system logs the deletion action, including the administrator's details and the personnel's information.   
10. The system removes or updates any references to the deleted personnel in related modules (e.g., assignment logs, case updates).   
11. The system displays a confirmation message indicating the successful deletion of the police personnel record.   
  
Alternative Flow:   
1. If the personnel ID is invalid or not found, the system displays an error message and prompts the administrator to enter a valid ID.   
2. If the administrator does not have authorization to delete the personnel record, the system denies access and logs the unauthorized attempt.   
3. If the system finds that the personnel is currently assigned to an active complaint or court case, it displays a warning and prevents the deletion until the assignments are reassigned or resolved.   
4. If the system fails to delete the personnel record due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the system fails to update the role configuration or other related modules, an error is logged, and the administrator is notified for follow-up.   
6. If the administrator cancels the deletion during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Create Court Case   
Use Case ID: UC-30   
Actors: Security Administrator, Criminal Police Personnel, Court Case Search   
  
Preconditions:   
1. A valid complaint or investigation record exists in the system with a valid complaint/investigation ID.   
2. The actor (Security Administrator or Criminal Police Personnel) has access to the court case creation system.   
3. The actor is authenticated and authorized to create court case records.   
4. The system is connected to the court case search module to ensure uniqueness and linkage.   
  
Postconditions:   
1. A new court case record is successfully created and stored in the system.   
2. The court case is linked to the associated complaint and investigation, if applicable.   
3. The creation action is logged for audit and traceability purposes.   
4. The court case is accessible to authorized personnel through the court case search module.   
  
Main Flow:   
1. The actor logs in to the court case management system.   
2. The actor navigates to the court case creation section.   
3. The actor selects the complaint or investigation by entering a valid complaint/investigation ID.   
4. The system retrieves the complaint or investigation details and confirms eligibility for court case creation.   
5. The actor inputs court case information (e.g., case type, filing date, involved parties, legal status).   
6. The system validates the input data for completeness and consistency with existing records.   
7. The system generates a unique court case ID and stores the new court case record in the database.   
8. The system links the court case to the associated complaint and investigation records.   
9. The system logs the creation action, including the actor's details and the court case information.   
10. The system displays a confirmation message indicating the successful creation of the court case.   
  
Alternative Flow:   
1. If the complaint or investigation ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the complaint or investigation is already linked to an existing court case, the system displays a warning and prevents duplicate court case creation.   
3. If the input data is incomplete or invalid, the system displays an error message and prompts the actor to correct the information.   
4. If the system fails to generate a court case ID, the security administrator is notified for manual intervention.   
5. If the system fails to link the court case to the complaint or investigation due to database constraints, an error is logged and the actor is notified for follow-up.   
6. If the actor is not authorized to create a court case, the system denies access and logs the unauthorized attempt.   
7. If the system fails to store the court case record due to database issues, it alerts the security administrator for manual resolution.   
8. If the actor cancels the court case creation during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: View Court Case   
Use Case ID: UC-31   
Actors: Security Administrator, Criminal Police Personnel, Court Case Search   
  
Preconditions:   
1. A court case has been registered in the system with a valid court case ID.   
2. The actor (Security Administrator, Criminal Police Personnel, or Court Case Search) has access to the court case viewing system.   
3. The actor is authenticated and authorized to view court case details.   
4. The system is connected to the court case database and any linked complaint or investigation records.   
  
Postconditions:   
1. The court case details are displayed to the authorized actor.   
2. The viewing action is logged in the system for audit and traceability purposes.   
3. If the court case is linked to a complaint or investigation, the related information is accessible to the actor.   
4. The system ensures that only authorized actors can view sensitive court case details.   
  
Main Flow:   
1. The actor logs in to the court case management system.   
2. The actor navigates to the court case viewing section.   
3. The actor enters or selects a valid court case ID.   
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, legal status, and any linked complaint or investigation records.   
6. The system logs the viewing action in the audit trail.   
7. The actor can optionally export or print the case details for official purposes.   
  
Alternative Flow:   
1. If the court case ID is invalid or not found, the system displays an error message and prompts the actor to enter a valid ID.   
2. If the actor does not have authorization to view the court case, the system denies access and logs the unauthorized attempt.   
3. If the system fails to retrieve the court case due to database issues, it alerts the security administrator for resolution.   
4. If the court case is linked to a complaint or investigation and the system fails to retrieve the related information, an error is logged, and the actor is notified for follow-up.   
5. If the actor cancels the viewing request during the confirmation step, the system returns to the previous screen without displaying the case details.  
  
Use Case Name: Delete Role   
Use Case ID: UC-32   
Actors: Security Administrator   
  
Preconditions:   
1. A role configuration exists in the system with a valid role ID.   
2. The actor (Security Administrator) has access to the role deletion system.   
3. The actor is authenticated and authorized to delete roles.   
4. The role to be deleted is not currently assigned to any active user accounts.   
  
Postconditions:   
1. The specified role is removed from the system.   
2. The deletion action is logged for audit and traceability purposes.   
3. The role configuration module is updated to reflect the deletion.   
4. If the role was referenced in any permissions or assignments, the system ensures these are either updated or invalidated to maintain data integrity.   
5. The system remains functional and secure after the deletion.   
  
Main Flow:   
1. The security administrator logs in to the role configuration management system.   
2. The administrator navigates to the role deletion section.   
3. The administrator enters or selects a valid role ID.   
4. The system retrieves and displays the role details for confirmation.   
5. The system checks whether the role is currently assigned to any user accounts.   
6. If the role is not assigned, the administrator confirms the deletion of the role.   
7. The system deletes the role from the role configuration database.   
8. The system updates the role configuration module to reflect the deletion.   
9. The system logs the deletion action with the administrator's details.   
10. The system displays a confirmation message indicating the successful deletion of the role.   
  
Alternative Flow:   
1. If the role ID is invalid or not found, the system displays an error message and prompts the administrator to enter a valid ID.   
2. If the administrator does not have authorization to delete the role, the system denies access and logs the unauthorized attempt.   
3. If the role is currently assigned to active user accounts, the system displays a warning and prevents deletion until all assignments are reassigned or removed.   
4. If the system fails to delete the role due to database constraints or errors, it alerts the security administrator for manual resolution.   
5. If the role deletion affects existing permissions or assignments and the system fails to update these references, an error is logged, and the administrator is notified for follow-up.   
6. If the administrator cancels the deletion during the confirmation step, the system returns to the previous screen without making any changes.  
  
Use Case Name: Create Configuration   
Use Case ID: UC-33   
Actors: Security Administrator   
  
Preconditions:   
1. The system configuration database is accessible and operational.   
2. The actor (Security Administrator) has access to the configuration creation system.   
3. The actor is authenticated and authorized to create system configurations.   
4. The role configuration module is connected and operational to ensure proper role-based access control.   
5. The system is not currently in a maintenance or update process that could conflict with configuration creation.   
  
Postconditions:   
1. A new configuration record is successfully created and stored in the system.   
2. The configuration is linked to the appropriate roles or system modules as defined.   
3. The creation action is logged in the system for audit and traceability purposes.   
4. The new configuration takes effect according to the system's update or activation rules.   
5. The system remains stable and secure after the configuration is created.   
  
Main Flow:   
1. The security administrator logs in to the system configuration management module.   
2. The administrator navigates to the configuration creation section.   
3. The system prompts the administrator to select a configuration type (e.g., access control, notification settings, case linkage rules).   
4. The administrator inputs the configuration parameters (e.g., role permissions, data retention policies, system alerts).   
5. The system validates the configuration data for consistency, correctness, and system compatibility.   
6. The system generates a unique configuration ID and stores the new configuration in the database.   
7. The system links the configuration to the relevant roles or modules if applicable.   
8. The system logs the configuration creation action, including the administrator's details and the configuration parameters.   
9. The system applies the new configuration based on predefined activation rules.   
10. The system displays a confirmation message indicating the successful creation of the configuration.   
  
Alternative Flow:   
1. If the configuration type is invalid or not supported, the system displays an error message and prompts the administrator to select a valid type.   
2. If the configuration parameters are incomplete or invalid, the system displays an error and prompts the administrator to correct the input.   
3. If the system fails to validate the configuration data due to conflicts or errors, it displays an error message and prevents the configuration from being created.   
4. If the system fails to generate a configuration ID, the security administrator is alerted for manual intervention.   
5. If the system fails to store the configuration in the database, it alerts the security administrator for manual resolution.   
6. If the system is in a maintenance or update process, the configuration creation is paused until the process is complete.   
7. If the administrator cancels the configuration creation during the confirmation step, the system returns to the previous screen without making any changes.