# 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。