# Functional Requirement

1. Functional Requirements  
  
1.1 Asset Registration Function   
Function ID: FR-01   
Description: Administrators can register new assets into the system by providing required details such as name, description, category, and department. The system validates the input, creates a new asset record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Asset details (name, description, category, department, etc.), valid administrator credentials.   
Output: New asset record in the database, audit log entry, email notification to stakeholders.  
  
1.2 View Asset Details Function   
Function ID: FR-02   
Description: Authenticated users or administrators can view detailed information of a specific asset, including its name, description, category, department, and usage status. The system checks permissions and logs the action in the audit log.   
Input: Selected asset ID, valid user or administrator credentials.   
Output: Displayed asset details, audit log entry.  
  
1.3 Modify Asset Information Function   
Function ID: FR-03   
Description: Administrators can modify the information of an existing asset, including name, description, category, and department. The system validates the input, updates the asset record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Updated asset details (name, description, category, department, etc.), valid administrator credentials.   
Output: Updated asset record in the database, audit log entry, email notification to stakeholders.  
  
1.4 Approve Asset Deletion Function   
Function ID: FR-04   
Description: Administrators can approve asset deletion requests. The system verifies the deletion request, removes the asset record from the database, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected asset deletion request, valid administrator credentials.   
Output: Deleted asset record, audit log entry, email notification to stakeholders.  
  
1.5 Assign Asset Permissions Function   
Function ID: FR-05   
Description: Administrators can assign specific permissions to users for a given asset. The system validates the user and permission, creates or updates a permission assignment record, logs the action in the audit log, and reflects the changes in the system.   
Input: Selected user ID, asset ID, permission level, valid administrator credentials.   
Output: Updated permission assignment record, audit log entry.  
  
1.6 Revoke Asset Permissions Function   
Function ID: FR-06   
Description: Administrators can revoke permissions assigned to a user for a given asset. The system validates the user and permission, updates the permission assignment record, logs the action in the audit log, and reflects the changes in the system.   
Input: Selected user ID, asset ID, permission to be revoked, valid administrator credentials.   
Output: Updated permission assignment record, audit log entry.  
  
1.7 Add User Function   
Function ID: FR-07   
Description: Administrators can add new users to the system by providing user details such as name, email, department, and permission level. The system validates the input, creates a new user record, assigns the user to a department, logs the action in the audit log, and optionally sends an email notification.   
Input: User details (name, email, department, permission level), valid administrator credentials.   
Output: New user record in the database, audit log entry, email notification to stakeholders.  
  
1.8 Delete User Function   
Function ID: FR-08   
Description: Administrators can delete a user from the system. The system validates the user, removes the user record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected user ID, valid administrator credentials.   
Output: Deleted user record, audit log entry, email notification to stakeholders.  
  
1.9 Modify User Profile Function   
Function ID: FR-09   
Description: Administrators can modify a user's profile information such as name, email, department, and permission level. The system validates the input, updates the user record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Updated user details (name, email, department, permission level), valid administrator credentials.   
Output: Updated user record in the database, audit log entry, email notification to stakeholders.  
  
1.10 View User Permissions Function   
Function ID: FR-10   
Description: Administrators can view the permissions assigned to a specific user. The system retrieves the permission records and logs the action in the audit log.   
Input: Selected user ID, valid administrator credentials.   
Output: Displayed list of user permissions, audit log entry.  
  
1.11 Create Administrator Function   
Function ID: FR-11   
Description: Administrators can create new administrator accounts by providing user information, department, and permission level. The system validates the input, creates a new administrator record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Administrator details (user ID, department, permission level), valid administrator credentials.   
Output: New administrator record in the database, audit log entry, email notification to stakeholders.  
  
1.12 Delete Administrator Function   
Function ID: FR-12   
Description: Administrators can delete an existing administrator account. The system validates the administrator, removes the record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected administrator ID, valid administrator credentials.   
Output: Deleted administrator record, audit log entry, email notification to stakeholders.  
  
1.13 Modify Administrator Role Function   
Function ID: FR-13   
Description: Administrators can modify the role or permission level of another administrator. The system validates the input, updates the administrator's role, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Updated administrator role or permission level, selected administrator ID, valid administrator credentials.   
Output: Updated administrator record in the database, audit log entry, email notification to stakeholders.  
  
1.14 View Department Assets Function   
Function ID: FR-14   
Description: Authenticated users or administrators can view the list of assets belonging to a specific department. The system checks permissions, retrieves the asset list, and logs the action in the audit log.   
Input: Selected department ID, valid user or administrator credentials.   
Output: Displayed list of assets, audit log entry.  
  
1.15 Update Department Information Function   
Function ID: FR-15   
Description: Administrators can update the information of a department, including name, description, and contact details. The system validates the input, updates the department record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Updated department details (name, description, contact details), valid administrator credentials.   
Output: Updated department record in the database, audit log entry, email notification to stakeholders.  
  
1.16 Add Asset Category Function   
Function ID: FR-16   
Description: Administrators can create new asset categories by providing name, description, and relevant attributes. The system validates the input, creates a new asset category record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Asset category details (name, description, attributes), valid administrator credentials.   
Output: New asset category record in the database, audit log entry, email notification to stakeholders.  
  
1.17 Modify Asset Category Function   
Function ID: FR-17   
Description: Administrators can update the information of an existing asset category. The system validates the input, updates the asset category record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Updated asset category details (name, description, attributes), valid administrator credentials.   
Output: Updated asset category record in the database, audit log entry, email notification to stakeholders.  
  
1.18 Delete Asset Category Function   
Function ID: FR-18   
Description: Administrators can delete an asset category if it is not currently in use by any asset. The system validates the category, removes the record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected asset category ID, valid administrator credentials.   
Output: Deleted asset category record, audit log entry, email notification to stakeholders.  
  
1.19 Record Asset Usage Function   
Function ID: FR-19   
Description: Users can record the usage of an asset by providing usage details such as start time, end time, and usage description. The system checks permissions, creates a new usage record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Asset ID, usage details (start time, end time, usage description), valid user credentials.   
Output: New usage record in the database, audit log entry, email notification to stakeholders.  
  
1.20 View Usage History Function   
Function ID: FR-20   
Description: Authenticated users or administrators can view the usage history of a specific asset. The system checks permissions, retrieves the usage records, and logs the action in the audit log.   
Input: Selected asset ID, valid user or administrator credentials.   
Output: Displayed list of usage records, audit log entry.  
  
1.21 Modify Usage Record Function   
Function ID: FR-21   
Description: Administrators or users with appropriate permissions can modify a usage record. The system validates the input, updates the usage record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected usage record ID, updated usage details, valid user or administrator credentials.   
Output: Updated usage record in the database, audit log entry, email notification to stakeholders.  
  
1.22 Delete Usage Record Function   
Function ID: FR-22   
Description: Administrators can delete a usage record. The system validates the input, removes the record, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected usage record ID, valid administrator credentials.   
Output: Deleted usage record, audit log entry, email notification to stakeholders.  
  
1.23 Generate Audit Log Function   
Function ID: FR-23   
Description: Administrators can generate an audit log entry for a specific system event or action. The system creates the log entry, logs the generation of the audit log as a meta-action, and sends an email notification to stakeholders.   
Input: Selected event or action, valid administrator credentials.   
Output: New audit log entry, audit log of the generation action, email notification to stakeholders.  
  
1.24 View Audit Log Function   
Function ID: FR-24   
Description: Authenticated users or administrators can view audit log entries. The system retrieves the logs, allows filtering or searching, and logs the viewing action in the audit log.   
Input: Filter/search criteria, valid user or administrator credentials.   
Output: Displayed audit log entries, audit log entry for the viewing action.  
  
1.25 Send Email Notification Function   
Function ID: FR-25   
Description: The system sends email notifications to stakeholders based on predefined events. The system generates content using templates, sends the notification via the configured email service, and logs the action in the audit log.   
Input: Event details (e.g., asset registration, user deletion), valid email service configuration.   
Output: Email notification sent to recipients, audit log entry.  
  
1.26 View Email Notification Function   
Function ID: FR-26   
Description: Authenticated users or administrators can view the content and details of an email notification. The system retrieves the notification from the database and logs the viewing action in the audit log.   
Input: Selected email notification ID, valid user or administrator credentials.   
Output: Displayed email notification details, audit log entry.  
  
1.27 Manage Permission Assignment Record Function   
Function ID: FR-27   
Description: Administrators can manage permission assignment records by creating, modifying, or deleting them. The system validates the input, updates the record in the database, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Permission assignment record details (user ID, asset ID, permission level), valid administrator credentials.   
Output: Updated permission assignment record, audit log entry, email notification to stakeholders.  
  
1.28 Manage Usage Approval Record Function   
Function ID: FR-28   
Description: Administrators or users can manage usage approval records by approving or rejecting them. The system validates the input, updates the approval status, logs the action in the audit log, and sends an email notification to stakeholders.   
Input: Selected usage approval record ID, approval/rejection status, valid administrator or user credentials.   
Output: Updated usage approval record, audit log entry, email notification to stakeholders.

# External Description

2. External Interfaces   
This section describes the system's interactions with external entities such as users, hardware, software, and communication channels. These interfaces are essential for the system's functionality, including asset and user management, audit logging, and email notifications.   
  
2.1 User Interface Output   
The user interface provides a graphical and intuitive way for administrators, users, and stakeholders to interact with the system. It includes the following outputs:   
  
- \*\*Display of asset details\*\*: After an asset is selected, the system displays detailed information such as name, description, category, department, and usage status. This is output through a web-based or desktop interface.   
- \*\*List of assets by department\*\*: Users or administrators can view a list of assets belonging to a specific department, including their names, descriptions, and status. This is output via a filtered or searchable interface.   
- \*\*List of user permissions\*\*: Administrators can view a list of permissions assigned to a specific user. This is output via a permissions management interface.   
- \*\*List of usage records\*\*: Users or administrators can view the usage history of an asset, including start time, end time, and usage description. This is output through a usage history interface.   
- \*\*List of audit log entries\*\*: Administrators can view a list of audit log entries, which includes system events and actions. The system supports filtering and searching for specific entries. This is output via an audit log interface.   
- \*\*Email notification details\*\*: Users or administrators can view the content and details of an email notification, including the recipient list, message body, and timestamp. This is output through a notification history interface.   
  
Each of these outputs is accompanied by an audit log entry, which is also displayed in the audit log interface. The interface must ensure appropriate permissions are enforced, and all actions taken by users or administrators are logged.   
  
2.2 Hardware Interface Output   
The system does not have direct hardware dependencies. Therefore, no hardware interfaces are required for the current scope of the system.   
  
2.3 Software Interface Output   
The system interacts with several internal and external software components to fulfill its functional requirements. The following are the key software interfaces:   
  
- \*\*Database Interface\*\*:   
 - \*\*Description\*\*: The system interacts with a centralized database to store and retrieve asset records, user records, permission assignments, usage records, and audit logs.   
 - \*\*Interaction Method\*\*: CRUD (Create, Read, Update, Delete) operations are performed via database queries and transactions.   
 - \*\*Data Format\*\*: Structured data in SQL format or NoSQL documents, depending on the database type.   
 - \*\*External Data Sources\*\*:   
 - Asset records (name, description, category, department, etc.)   
 - User records (name, email, department, permission level)   
 - Permission assignment records (user ID, asset ID, permission level)   
 - Usage records (start time, end time, usage description)   
 - Audit log entries (action performed, timestamp, user ID, asset ID, etc.)   
  
- \*\*Email Service Interface\*\*:   
 - \*\*Description\*\*: The system communicates with an external email service to send notifications to stakeholders when predefined events occur, such as asset registration, modification, deletion, or user changes.   
 - \*\*Interaction Method\*\*: The system generates email content using predefined templates and sends the notification via an API or SMTP interface.   
 - \*\*Data Format\*\*: Email messages are formatted in plain text or HTML, with structured headers and metadata.   
 - \*\*External Data Sources\*\*:   
 - Stakeholder email addresses   
 - Email templates for notifications   
 - System event details (e.g., asset or user modification)   
  
2.4 Communication Interface Output   
The system communicates with external entities through the following interfaces:   
  
- \*\*Email Notifications\*\*:   
 - \*\*Description\*\*: The system sends email notifications to stakeholders to inform them of changes to assets, users, permissions, or other system events.   
 - \*\*Interaction Method\*\*: Email is sent via a configured email service using SMTP or a REST API. The system uses templates to generate the email content dynamically.   
 - \*\*Inputs/Outputs\*\*:   
 - Inputs: Event details (e.g., asset registration, user deletion), recipient email addresses, and email templates.   
 - Outputs: Email notification sent to recipients, audit log entry for the notification.   
  
- \*\*Web-based Communication\*\*:   
 - \*\*Description\*\*: The system supports access via a web interface, allowing users and administrators to perform actions such as viewing assets, modifying records, or managing permissions.   
 - \*\*Interaction Method\*\*: HTTP/HTTPS protocols are used for communication between the client and server. The system provides a RESTful API for integration with external tools.   
 - \*\*Inputs/Outputs\*\*:   
 - Inputs: User credentials, selected asset/user IDs, and updated information.   
 - Outputs: Displayed data, status responses, and audit log entries.   
  
- \*\*Audit Log Communication\*\*:   
 - \*\*Description\*\*: The system logs all user and administrator actions into an audit log, including the creation, modification, and deletion of assets, users, permissions, and usage records.   
 - \*\*Interaction Method\*\*: The audit log is stored in the database and is accessible via a dedicated interface for viewing.   
 - \*\*Inputs/Outputs\*\*:   
 - Inputs: Action performed, user ID, timestamp, and related asset or user IDs.   
 - Outputs: Audit log entry stored in the database, displayed via the audit log interface.   
  
Each communication interface is designed to ensure secure and reliable data exchange, with audit logs capturing all interactions for traceability and compliance.