# 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.