项目文档

# 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.

# Use Case

Use Case Name: Asset Registration   
Use Case ID: UC-01   
Actors: Administrator, Department, Asset Category, Permission, Asset, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to register assets.   
2. The department for which the asset is being registered exists in the system.   
3. The asset category for the asset is already defined in the system.   
4. The system is accessible and functioning properly.   
  
Postconditions:   
1. A new asset record is created in the system.   
2. An audit log entry is generated to document the asset registration.   
3. An email notification is sent to the relevant stakeholders or users.   
  
Main Flow:   
1. The administrator selects the "Asset Registration" option from the system menu.   
2. The system displays the asset registration form.   
3. The administrator enters the asset details, including name, description, category, and department.   
4. The system validates the input data and ensures all mandatory fields are filled.   
5. The system creates a new asset record with the provided information.   
6. The system updates the audit log with the registration details.   
7. The system sends an email notification to the department and administrator confirming the asset registration.   
8. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected department or asset category does not exist, the system displays a warning message and prevents the asset from being registered until the correct selections are made.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: View Asset Details   
Use Case ID: UC-02   
Actors: User, Administrator, Asset, Department, Asset Category, Permission, Audit Log   
  
Preconditions:   
1. The user or administrator has been authenticated and has the necessary permission to view asset details.   
2. The asset to be viewed exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user or administrator is presented with the detailed information of the selected asset.   
2. An audit log entry is generated to document the viewing of the asset details.   
  
Main Flow:   
1. The user or administrator selects an asset from the asset list.   
2. The system checks the permissions to ensure the user has access to view the asset details.   
3. The system retrieves the asset details, including name, description, category, and department.   
4. The system displays the asset details in a dedicated view.   
5. The system logs the viewing action into the audit log.   
  
Alternative Flow:   
1. If the user does not have the required permission, the system displays an access denied message.   
2. If the selected asset does not exist, the system displays an error message and prompts the user to select a valid asset.   
3. If the system fails to retrieve the asset details, the system displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: Modify Asset Information   
Use Case ID: UC-03   
Actors: Administrator, Asset, Department, Asset Category, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to modify asset information.   
2. The asset to be modified exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The asset information is updated in the system.   
2. An audit log entry is generated to document the modification.   
3. An email notification is sent to the relevant stakeholders or users regarding the change.   
  
Main Flow:   
1. The administrator selects the "Modify Asset Information" option from the system menu.   
2. The system displays a list of existing assets.   
3. The administrator selects an asset to modify.   
4. The system displays the asset details in an editable form.   
5. The administrator updates the asset information, such as name, description, category, or department.   
6. The system validates the updated data and ensures all mandatory fields are filled.   
7. The system updates the asset record with the new information.   
8. The system logs the modification into the audit log.   
9. The system sends an email notification to the department and administrator confirming the asset modification.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the updated data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected department or asset category does not exist, the system displays a warning message and prevents the modification until the correct selections are made.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Approve Asset Deletion   
Use Case ID: UC-04   
Actors: Administrator, Asset, Department, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to delete assets.   
2. The asset to be deleted exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The asset record is deleted from the system.   
2. An audit log entry is generated to document the asset deletion.   
3. An email notification is sent to the relevant stakeholders or users regarding the deletion.   
  
Main Flow:   
1. The administrator selects the "Approve Asset Deletion" option from the system menu.   
2. The system displays a list of pending asset deletion requests.   
3. The administrator selects a specific asset deletion request for approval.   
4. The system confirms the asset details and the requestor's information.   
5. The administrator confirms the approval of the deletion.   
6. The system deletes the selected asset record from the database.   
7. The system logs the deletion action into the audit log.   
8. The system sends an email notification to the department and administrator confirming the deletion.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator does not have the required permission, the system displays an access denied message.   
2. If the selected asset does not exist, the system displays an error message and prompts the administrator to select a valid asset.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Assign Asset Permissions   
Use Case ID: UC-05   
Actors: Administrator, Asset, Department, User, Permission, Audit Log   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to assign asset permissions.   
2. The asset for which permissions are being assigned exists in the system.   
3. The department and user involved are already registered in the system.   
4. The system is accessible and functioning properly.   
  
Postconditions:   
1. The selected user is granted the specified permission to the asset.   
2. An audit log entry is generated to document the permission assignment.   
3. The permission changes are reflected in the system for future access control.   
  
Main Flow:   
1. The administrator selects the "Assign Asset Permissions" option from the system menu.   
2. The system displays a list of assets available for permission assignment.   
3. The administrator selects an asset and views the current permissions assigned to it.   
4. The administrator selects a user from the system user list.   
5. The administrator chooses the appropriate permission level for the selected user.   
6. The system validates the selected user and permission.   
7. The system updates the asset's permission records to include the new assignment.   
8. The system logs the permission assignment action into the audit log.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the selected user does not exist, the system displays an error message and prompts the administrator to choose a valid user.   
2. If the selected permission is invalid or not applicable to the asset, the system displays a warning message and prevents the assignment.   
3. If the system fails to update the permissions or log the action, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Revoke Asset Permissions   
Use Case ID: UC-06   
Actors: Administrator, Asset, Department, User, Permission, Audit Log   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to revoke asset permissions.   
2. The asset for which permissions are being revoked exists in the system.   
3. The user to whom the permission was assigned is registered in the system.   
4. The permission to be revoked is currently assigned to the user for the selected asset.   
5. The system is accessible and functioning properly.   
  
Postconditions:   
1. The selected permission is successfully removed from the user for the specified asset.   
2. An audit log entry is generated to document the permission revocation.   
3. The permission changes are reflected in the system for future access control.   
  
Main Flow:   
1. The administrator selects the "Revoke Asset Permissions" option from the system menu.   
2. The system displays a list of assets with their associated permissions.   
3. The administrator selects an asset and views the list of users with permissions assigned.   
4. The administrator selects a user and the specific permission to be revoked.   
5. The system validates the selected user and permission against the asset's current configuration.   
6. The system removes the selected permission from the user for the asset.   
7. The system logs the revocation action into the audit log.   
8. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the selected user does not have the specified permission for the asset, the system displays an error message and prompts the administrator to choose a valid permission.   
2. If the selected permission is invalid or not applicable to the asset, the system displays a warning message and prevents the revocation.   
3. If the system fails to update the permissions or log the action, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Add User   
Use Case ID: UC-07   
Actors: Administrator, User, Department, Permission, Audit Log   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to add users.   
2. The department to which the user will be assigned exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. A new user record is created in the system.   
2. The user is assigned to the specified department and has the defined permissions.   
3. An audit log entry is generated to document the user addition.   
  
Main Flow:   
1. The administrator selects the "Add User" option from the system menu.   
2. The system displays the user registration form.   
3. The administrator enters the user's details, including name, email, department, and permission level.   
4. The system validates the input data and ensures all mandatory fields are filled.   
5. The system creates a new user record with the provided information.   
6. The system assigns the user to the selected department and applies the specified permissions.   
7. The system logs the user addition action into the audit log.   
8. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected department does not exist, the system displays a warning message and prevents the user from being added until a valid department is selected.   
3. If the system fails to log the action, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Delete User   
Use Case ID: UC-08   
Actors: Administrator, User, Department, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to delete users.   
2. The user to be deleted exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user record is deleted from the system.   
2. An audit log entry is generated to document the user deletion.   
3. An email notification is sent to the relevant stakeholders or users regarding the deletion.   
  
Main Flow:   
1. The administrator selects the "Delete User" option from the system menu.   
2. The system displays a list of existing users.   
3. The administrator selects a specific user to delete.   
4. The system confirms the user's details and their associated department and permissions.   
5. The administrator confirms the deletion of the user.   
6. The system deletes the selected user record from the database.   
7. The system logs the deletion action into the audit log.   
8. The system sends an email notification to the department and administrator confirming the user deletion.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the administrator does not have the required permission, the system displays an access denied message.   
2. If the selected user does not exist, the system displays an error message and prompts the administrator to select a valid user.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Modify User Profile   
Use Case ID: UC-09   
Actors: Administrator, User, Department, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to modify user profiles.   
2. The user whose profile is to be modified exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user's profile information is updated in the system.   
2. An audit log entry is generated to document the modification.   
3. An email notification is sent to the user and administrator confirming the profile changes.   
  
Main Flow:   
1. The administrator selects the "Modify User Profile" option from the system menu.   
2. The system displays a list of existing users.   
3. The administrator selects a specific user to modify.   
4. The system retrieves the current profile information and displays it in an editable form.   
5. The administrator updates the user's details, such as name, email, department, or permission level.   
6. The system validates the updated data and ensures all mandatory fields are filled.   
7. The system updates the user record with the new information.   
8. The system logs the profile modification into the audit log.   
9. The system sends an email notification to the user and administrator confirming the modification.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the updated data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected department does not exist, the system displays a warning message and prevents the modification until a valid department is selected.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: View User Permissions   
Use Case ID: UC-10   
Actors: Administrator, User, Permission, Audit Log   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to view user permissions.   
2. The user whose permissions are to be viewed exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The administrator is presented with the list of permissions assigned to the selected user.   
2. An audit log entry is generated to document the viewing of user permissions.   
  
Main Flow:   
1. The administrator selects the "View User Permissions" option from the system menu.   
2. The system displays a list of users in the system.   
3. The administrator selects a specific user to view their permissions.   
4. The system retrieves and displays the list of permissions currently assigned to the selected user.   
5. The system logs the viewing action into the audit log.   
6. The system displays the permissions summary to the administrator.   
  
Alternative Flow:   
1. If the selected user does not exist, the system displays an error message and prompts the administrator to choose a valid user.   
2. If the administrator does not have the required permission to view user permissions, the system displays an access denied message.   
3. If the system fails to retrieve or display the permissions, the system logs the error and displays a message to the administrator for troubleshooting.  
  
Use Case Name: Create Administrator   
Use Case ID: UC-11   
Actors: Administrator, User, Department, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to create new administrators.   
2. The user to be assigned as an administrator is already registered in the system.   
3. The department to which the administrator will be assigned exists in the system.   
4. The system is accessible and functioning properly.   
  
Postconditions:   
1. A new administrator record is created in the system.   
2. The administrator is assigned to the specified department and has the defined permissions.   
3. An audit log entry is generated to document the creation of the administrator.   
4. An email notification is sent to the new administrator and relevant stakeholders.   
  
Main Flow:   
1. The administrator selects the "Create Administrator" option from the system menu.   
2. The system displays the administrator creation form.   
3. The administrator enters the details for the new administrator, including user information, department, and permission level.   
4. The system validates the input data and ensures all mandatory fields are filled.   
5. The system creates a new administrator record with the provided information.   
6. The system assigns the new administrator to the selected department and applies the specified permissions.   
7. The system logs the administrator creation action into the audit log.   
8. The system sends an email notification to the new administrator and the current administrator confirming the creation.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected department does not exist, the system displays a warning message and prevents the administrator from being created until a valid department is selected.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Delete Administrator   
Use Case ID: UC-12   
Actors: Administrator, User, Department, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to delete administrators.   
2. The administrator to be deleted exists in the system and is associated with a department.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The administrator record is deleted from the system.   
2. An audit log entry is generated to document the deletion.   
3. An email notification is sent to the relevant stakeholders or users regarding the deletion.   
  
Main Flow:   
1. The administrator selects the "Delete Administrator" option from the system menu.   
2. The system displays a list of existing administrators.   
3. The administrator selects a specific administrator to delete.   
4. The system confirms the selected administrator's details and their associated department and permissions.   
5. The administrator confirms the deletion of the target administrator.   
6. The system deletes the selected administrator record from the database.   
7. The system logs the deletion action into the audit log.   
8. The system sends an email notification to the department and current administrator confirming the deletion.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the selected administrator does not exist, the system displays an error message and prompts the administrator to choose a valid one.   
2. If the current user does not have the required permission to delete administrators, the system displays an access denied message.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Modify Administrator Role   
Use Case ID: UC-13   
Actors: Administrator, User, Department, Permission, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to modify administrator roles.   
2. The target administrator exists in the system and is associated with a department.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The target administrator's role or permissions are updated in the system.   
2. An audit log entry is generated to document the role modification.   
3. An email notification is sent to the target administrator and relevant stakeholders regarding the role change.   
  
Main Flow:   
1. The administrator selects the "Modify Administrator Role" option from the system menu.   
2. The system displays a list of existing administrators.   
3. The administrator selects a specific administrator to modify their role.   
4. The system retrieves and displays the current role and permissions of the selected administrator.   
5. The administrator updates the role or permission level for the selected administrator.   
6. The system validates the updated role and permission against the system's configuration.   
7. The system updates the administrator's role and permission in the database.   
8. The system logs the modification into the audit log.   
9. The system sends an email notification to the modified administrator and the current administrator confirming the change.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the updated role or permission is invalid or not applicable, the system displays a warning message and prevents the modification.   
2. If the selected administrator does not exist, the system displays an error message and prompts the administrator to choose a valid one.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: View Department Assets   
Use Case ID: UC-14   
Actors: User, Administrator, Department, Asset, Asset Category, Permission, Audit Log   
  
Preconditions:   
1. The user or administrator has been authenticated and has the necessary permission to view department assets.   
2. The department whose assets are to be viewed exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user or administrator is presented with a list of assets belonging to the selected department.   
2. An audit log entry is generated to document the viewing of department assets.   
  
Main Flow:   
1. The user or administrator selects the "View Department Assets" option from the system menu.   
2. The system displays a list of departments in the system.   
3. The user or administrator selects a specific department to view its assets.   
4. The system checks the permissions to ensure the user has access to view the department's assets.   
5. The system retrieves and displays the list of assets associated with the selected department.   
6. The system logs the viewing action into the audit log.   
  
Alternative Flow:   
1. If the user does not have the required permission, the system displays an access denied message.   
2. If the selected department does not exist, the system displays an error message and prompts the user to select a valid department.   
3. If the system fails to retrieve the asset list, the system displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: Update Department Information   
Use Case ID: UC-15   
Actors: Administrator, Department, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to update department information.   
2. The department whose information is to be updated exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The department information is updated in the system.   
2. An audit log entry is generated to document the update.   
3. An email notification is sent to the relevant stakeholders or users regarding the change.   
  
Main Flow:   
1. The administrator selects the "Update Department Information" option from the system menu.   
2. The system displays a list of departments.   
3. The administrator selects a department to update.   
4. The system retrieves and displays the current department details in an editable form.   
5. The administrator modifies the department information, such as name, description, or contact details.   
6. The system validates the updated data and ensures all mandatory fields are filled.   
7. The system updates the department record with the new information.   
8. The system logs the update action into the audit log.   
9. The system sends an email notification to the department and administrator confirming the update.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the updated data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected department does not exist, the system displays an error message and prompts the administrator to choose a valid department.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Add Asset Category   
Use Case ID: UC-16   
Actors: Administrator, Asset Category, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to add asset categories.   
2. The system is accessible and functioning properly.   
  
Postconditions:   
1. A new asset category is added to the system.   
2. An audit log entry is generated to document the addition of the asset category.   
3. An email notification is sent to the administrator and relevant stakeholders confirming the addition.   
  
Main Flow:   
1. The administrator selects the "Add Asset Category" option from the system menu.   
2. The system displays the asset category creation form.   
3. The administrator enters the category details, such as name, description, and any relevant attributes.   
4. The system validates the input data and ensures all mandatory fields are filled.   
5. The system creates a new asset category record with the provided information.   
6. The system logs the creation action into the audit log.   
7. The system sends an email notification to the administrator and stakeholders confirming the category addition.   
8. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Modify Asset Category   
Use Case ID: UC-17   
Actors: Administrator, Asset Category, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to modify asset categories.   
2. The asset category to be modified exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The asset category information is updated in the system.   
2. An audit log entry is generated to document the modification.   
3. An email notification is sent to the administrator and relevant stakeholders confirming the category modification.   
  
Main Flow:   
1. The administrator selects the "Modify Asset Category" option from the system menu.   
2. The system displays a list of existing asset categories.   
3. The administrator selects a specific asset category to modify.   
4. The system retrieves and displays the current category details in an editable form.   
5. The administrator updates the category information, such as name, description, or attributes.   
6. The system validates the updated data and ensures all mandatory fields are filled.   
7. The system updates the asset category record with the new information.   
8. The system logs the modification into the audit log.   
9. The system sends an email notification to the administrator and stakeholders confirming the modification.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the updated data is invalid or incomplete, the system displays an error message and prompts the administrator to correct the information.   
2. If the selected asset category does not exist, the system displays an error message and prompts the administrator to choose a valid category.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Delete Asset Category   
Use Case ID: UC-18   
Actors: Administrator, Asset Category, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to delete asset categories.   
2. The asset category to be deleted exists in the system and is not currently assigned to any asset.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The asset category is deleted from the system.   
2. An audit log entry is generated to document the deletion of the asset category.   
3. An email notification is sent to the administrator and relevant stakeholders confirming the deletion.   
  
Main Flow:   
1. The administrator selects the "Delete Asset Category" option from the system menu.   
2. The system displays a list of existing asset categories.   
3. The administrator selects a specific asset category to delete.   
4. The system checks whether the selected category is currently in use by any asset.   
5. If no assets are using the category, the system confirms the deletion request.   
6. The administrator confirms the deletion of the selected asset category.   
7. The system deletes the asset category record from the database.   
8. The system logs the deletion action into the audit log.   
9. The system sends an email notification to the administrator and stakeholders confirming the category deletion.   
10. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the selected asset category is currently assigned to one or more assets, the system displays a warning message and prevents deletion until the category is no longer in use.   
2. If the selected asset category does not exist, the system displays an error message and prompts the administrator to choose a valid category.   
3. If the administrator does not have the required permission, the system displays an access denied message.   
4. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Record Asset Usage   
Use Case ID: UC-19   
Actors: User, Asset, Department, Audit Log, Email Notification   
Preconditions:   
1. The user has been authenticated and has the necessary permission to use the asset.   
2. The asset exists in the system and is available for usage.   
3. The department to which the asset is assigned exists in the system.   
4. The system is accessible and functioning properly.   
  
Postconditions:   
1. A new usage record is created for the selected asset.   
2. An audit log entry is generated to document the asset usage.   
3. An email notification is sent to the relevant stakeholders or users regarding the usage.   
  
Main Flow:   
1. The user selects the "Record Asset Usage" option from the system interface.   
2. The system displays a list of available assets for usage.   
3. The user selects a specific asset to record usage for.   
4. The system checks if the user has the required permission to use the asset.   
5. The system prompts the user to enter usage details (e.g., start time, end time, usage description).   
6. The system validates the input data and ensures all mandatory fields are filled.   
7. The system creates a new asset usage record with the provided information.   
8. The system logs the usage action into the audit log.   
9. The system sends an email notification to the department and administrator confirming the usage.   
10. The system displays a confirmation message to the user.   
  
Alternative Flow:   
1. If the user does not have the required permission to use the asset, the system displays an access denied message.   
2. If the selected asset does not exist, the system displays an error message and prompts the user to select a valid asset.   
3. If the input data is invalid or incomplete, the system displays an error message and prompts the user to correct the information.   
4. If the system fails to send the email notification, the user is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: View Usage History   
Use Case ID: UC-20   
Actors: User, Administrator, Usage Record, Asset, Department, Audit Log   
Preconditions:   
1. The user or administrator has been authenticated and has the necessary permission to view usage history.   
2. The asset for which usage history is to be viewed exists in the system.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user or administrator is presented with the usage history of the selected asset.   
2. An audit log entry is generated to document the viewing of the usage history.   
  
Main Flow:   
1. The user or administrator selects the "View Usage History" option from the system menu.   
2. The system displays a list of assets in the system.   
3. The user or administrator selects a specific asset to view its usage history.   
4. The system checks the permissions to ensure the user has access to view the usage history of the asset.   
5. The system retrieves and displays the usage records for the selected asset, including details such as start time, end time, and usage description.   
6. The system logs the viewing action into the audit log.   
  
Alternative Flow:   
1. If the user does not have the required permission, the system displays an access denied message.   
2. If the selected asset does not exist, the system displays an error message and prompts the user to select a valid asset.   
3. If the system fails to retrieve the usage records, the system logs the error and displays a message to the user or administrator for troubleshooting.  
  
Use Case Name: Modify Usage Record   
Use Case ID: UC-21   
Actors: Administrator, User, Usage Record, Asset, Department, Audit Log, Email Notification   
Preconditions:   
1. The administrator or user has been authenticated and has the necessary permission to modify usage records.   
2. The usage record to be modified exists in the system and is associated with a valid asset.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The usage record is updated with the new information.   
2. An audit log entry is generated to document the modification of the usage record.   
3. An email notification is sent to the relevant stakeholders or users regarding the modification.   
  
Main Flow:   
1. The administrator or user selects the "Modify Usage Record" option from the system menu.   
2. The system displays a list of existing usage records.   
3. The administrator or user selects a specific usage record to modify.   
4. The system retrieves and displays the current usage record details in an editable form.   
5. The administrator or user updates the usage information, such as start time, end time, or usage description.   
6. The system validates the updated data and ensures all mandatory fields are filled.   
7. The system updates the usage record with the new information.   
8. The system logs the modification into the audit log.   
9. The system sends an email notification to the department and administrator confirming the modification.   
10. The system displays a confirmation message to the user or administrator.   
  
Alternative Flow:   
1. If the updated data is invalid or incomplete, the system displays an error message and prompts the user or administrator to correct the information.   
2. If the selected usage record does not exist, the system displays an error message and prompts the user to select a valid usage record.   
3. If the user or administrator does not have the required permission, the system displays an access denied message.   
4. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Delete Usage Record   
Use Case ID: UC-22   
Actors: Administrator, Usage Record, Asset, Department, Audit Log, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to delete usage records.   
2. The usage record to be deleted exists in the system and is associated with a valid asset.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The selected usage record is deleted from the system.   
2. An audit log entry is generated to document the deletion of the usage record.   
3. An email notification is sent to the relevant stakeholders or users regarding the deletion.   
  
Main Flow:   
1. The administrator selects the "Delete Usage Record" option from the system menu.   
2. The system displays a list of usage records in the system.   
3. The administrator selects a specific usage record to delete.   
4. The system confirms the details of the selected usage record and its associated asset.   
5. The administrator confirms the deletion of the selected usage record.   
6. The system deletes the usage record from the database.   
7. The system logs the deletion action into the audit log.   
8. The system sends an email notification to the department and administrator confirming the deletion.   
9. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the selected usage record does not exist, the system displays an error message and prompts the administrator to choose a valid one.   
2. If the administrator does not have the required permission, the system displays an access denied message.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Generate Audit Log   
Use Case ID: UC-23   
Actors: Administrator, Audit Log, Asset, Department, User, Permission, Usage Record, Email Notification   
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to generate audit logs.   
2. The system contains at least one recorded event that requires audit logging.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. A new audit log entry is generated for the specified event or action.   
2. The audit log is updated in the system.   
3. An email notification is sent to the administrator and relevant stakeholders confirming the audit log generation.   
  
Main Flow:   
1. The administrator selects the "Generate Audit Log" option from the system menu.   
2. The system displays a list of events or actions that can be audited (e.g., asset registration, user modification).   
3. The administrator selects the specific event or action to generate an audit log for.   
4. The system retrieves the relevant details of the selected event, including timestamps, actor, and changes made.   
5. The system creates a new audit log entry with the retrieved information.   
6. The system logs the audit log generation into the audit log itself as a meta-action.   
7. The system sends an email notification to the administrator and stakeholders confirming the audit log entry.   
8. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the selected event or action does not exist in the system, the system displays an error message and prompts the administrator to choose a valid event.   
2. If the administrator does not have the required permission, the system displays an access denied message.   
3. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: View Audit Log   
Use Case ID: UC-24   
Actors: Administrator, User, Audit Log   
Preconditions:   
1. The user or administrator has been authenticated and has the necessary permission to view audit logs.   
2. The audit log contains at least one entry that can be viewed.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user or administrator is presented with the audit log entries.   
2. An audit log entry is generated to document the viewing of the audit log.   
  
Main Flow:   
1. The user or administrator selects the "View Audit Log" option from the system menu.   
2. The system displays a list of available audit log entries.   
3. The user or administrator filters or searches for specific entries if needed.   
4. The system retrieves and displays the selected audit log entries, including event type, timestamp, actor, and details.   
5. The system logs the viewing action into the audit log.   
  
Alternative Flow:   
1. If the user or administrator does not have the required permission, the system displays an access denied message.   
2. If no audit log entries are found based on the search/filter criteria, the system displays a message indicating no results.   
3. If the system fails to retrieve the audit log entries, it displays an error message and logs the issue for troubleshooting.  
  
Use Case Name: Send Email Notification   
Use Case ID: UC-25   
Actors: System, Email Notification, User, Administrator, Department, Asset, Audit Log   
Preconditions:   
1. The system has access to an email service or SMTP server.   
2. The email notification feature is configured and enabled in the system.   
3. The recipient email addresses are valid and stored in the system.   
4. The system has a message template for the notification.   
5. The system is accessible and functioning properly.   
  
Postconditions:   
1. An email notification is successfully sent to the intended recipients.   
2. The system logs the email notification action in the audit log.   
3. The recipients are informed of the relevant system event or action.   
  
Main Flow:   
1. The system triggers the "Send Email Notification" use case in response to a specific event (e.g., asset registration, user deletion).   
2. The system identifies the recipients based on the event, such as the department head, administrator, or user.   
3. The system generates the email content using the appropriate template and includes event-specific details (e.g., asset name, user information).   
4. The system sends the email notification to the identified recipients via the configured email service.   
5. The system logs the email notification action in the audit log, including the timestamp and recipients.   
6. The system confirms the successful delivery of the email notification.   
  
Alternative Flow:   
1. If the email service is not available or there is a network issue, the system logs the failure and displays an error message to the relevant actor.   
2. If the recipient email address is invalid or missing, the system skips the notification for that recipient and logs a warning.   
3. If the email template is missing or cannot be processed, the system displays an error message and does not send the notification.   
4. If the system fails to log the email notification action, it logs the error for troubleshooting and alerts the administrator.  
  
Use Case Name: View Email Notification   
Use Case ID: UC-26   
Actors: User, Administrator, Email Notification, Audit Log   
Preconditions:   
1. The user or administrator has been authenticated and has the necessary permission to view email notifications.   
2. The email notification to be viewed exists in the system and is associated with a valid event or action.   
3. The system is accessible and functioning properly.   
  
Postconditions:   
1. The user or administrator is presented with the content and details of the selected email notification.   
2. An audit log entry is generated to document the viewing of the email notification.   
  
Main Flow:   
1. The user or administrator selects the "View Email Notification" option from the system menu.   
2. The system displays a list of previously sent email notifications.   
3. The user or administrator selects a specific email notification to view.   
4. The system retrieves and displays the notification details, including recipient, timestamp, and message content.   
5. The system logs the viewing action into the audit log.   
  
Alternative Flow:   
1. If the selected email notification does not exist, the system displays an error message and prompts the user to select a valid notification.   
2. If the user or administrator does not have the required permission, the system displays an access denied message.   
3. If the system fails to retrieve the email notification, it logs the error and displays a message to the user or administrator for troubleshooting.  
  
Use Case Name: Manage Permission Assignment Record   
Use Case ID: UC-27   
Actors: Administrator, User, Asset, Department, Permission, Audit Log, Email Notification   
  
Preconditions:   
1. The administrator has been authenticated and has the necessary permission to manage permission assignment records.   
2. The user, asset, and department involved in the permission assignment are already registered in the system.   
3. The permission to be assigned or modified exists in the system.   
4. The system is accessible and functioning properly.   
  
Postconditions:   
1. The permission assignment record is either created, modified, or deleted based on the administrator's action.   
2. An audit log entry is generated to document the change to the permission assignment record.   
3. An email notification is sent to the relevant stakeholders or users regarding the change.   
  
Main Flow:   
1. The administrator selects the "Manage Permission Assignment Record" option from the system menu.   
2. The system displays a list of existing permission assignment records, including the user, asset, department, and assigned permission.   
3. The administrator chooses an action (e.g., add, modify, or delete) for a specific permission assignment record.   
4. If adding a new record, the administrator selects a user, an asset, a department, and assigns a permission level.   
5. If modifying a record, the administrator selects an existing permission assignment and updates the permission level or other relevant details.   
6. If deleting a record, the administrator selects an existing permission assignment and confirms the deletion.   
7. The system validates the input data and checks for system consistency (e.g., user and asset existence, valid permission level).   
8. The system updates the permission assignment record in the database accordingly (create, modify, or delete).   
9. The system logs the action (create, modify, or delete) into the audit log.   
10. The system sends an email notification to the administrator, the user involved, and the department regarding the change.   
11. The system displays a confirmation message to the administrator.   
  
Alternative Flow:   
1. If the input data is invalid or incomplete (e.g., user or asset not found, invalid permission level), the system displays an error message and prompts the administrator to correct the information.   
2. If the administrator does not have the required permission to perform the selected action, the system displays an access denied message.   
3. If the system fails to update the permission assignment record or log the action, the administrator is informed of the failure, and the system logs the error for troubleshooting.   
4. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.  
  
Use Case Name: Manage Usage Approval Record   
Use Case ID: UC-28   
Actors: Administrator, User, Usage Approval Record, Asset, Department, Audit Log, Email Notification   
  
Preconditions:   
1. The administrator or user has been authenticated and has the necessary permission to manage usage approval records.   
2. The system contains at least one usage request that requires approval.   
3. The asset associated with the usage request exists in the system.   
4. The department to which the asset is assigned exists in the system.   
5. The system is accessible and functioning properly.   
  
Postconditions:   
1. The usage approval record is either created, modified, or deleted based on the administrator's or user's action.   
2. An audit log entry is generated to document the change to the usage approval record.   
3. An email notification is sent to the relevant stakeholders or users regarding the approval status change.   
  
Main Flow:   
1. The administrator or user selects the "Manage Usage Approval Record" option from the system menu.   
2. The system displays a list of pending or existing usage approval records.   
3. The administrator or user selects a specific usage approval record to manage.   
4. If approving a record, the system verifies the user or administrator has the authority to approve the selected usage request.   
5. The system updates the status of the usage approval record to "approved" or "rejected" based on the decision.   
6. The system logs the approval or rejection action into the audit log, including the actor and timestamp.   
7. The system sends an email notification to the user who requested the usage, the department, and the administrator confirming the approval status change.   
8. The system displays a confirmation message to the administrator or user indicating the action was completed.   
  
Alternative Flow:   
1. If the selected usage approval record does not exist, the system displays an error message and prompts the administrator or user to select a valid record.   
2. If the user or administrator does not have the required permission to approve or reject a usage request, the system displays an access denied message.   
3. If the system fails to update the usage approval record or log the action, the administrator is informed of the failure, and the system logs the error for troubleshooting.   
4. If the system fails to send the email notification, the administrator is informed of the failure, and the system logs the error for troubleshooting.