项目文档

# Functional Requirement

# 1. Functional Requirements  
  
## 1.1 Asset Lifecycle Management Function   
Function ID: FR-01   
Description: Manage the full lifecycle of an asset, including stages such as acquisition, deployment, maintenance, and decommissioning. The system must support lifecycle updates with appropriate validation, approval workflow, and audit trail.   
Input: AssetID, Stage, Notes, UserID   
Output: Updated AssetLifeCycle record in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.2 Asset Usage Tracking Function   
Function ID: FR-02   
Description: Track and record asset usage by users, including usage date, duration, and purpose. The system must validate user permissions and initiate approval workflows if required.   
Input: AssetID, UserID, UsageDate, UsageDuration, UsagePurpose   
Output: AssetUsage record in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.3 Asset Report Generation Function   
Function ID: FR-03   
Description: Generate reports based on asset data, including lifecycle, usage, and summary reports. The system must allow report customization through filters and options.   
Input: ReportType, Filters (e.g., time range, asset category), UserID   
Output: ReportAnalysis record in the Database, Report file (CSV, Excel, PDF), EmailNotification with report, AuditTrail record  
  
## 1.4 Asset Data Analysis Function   
Function ID: FR-04   
Description: Analyze asset data to produce insights such as performance, usage trends, and lifecycle efficiency. The system must support viewing and downloading of analysis results.   
Input: AssetID, AnalysisType, UserID   
Output: ReportAnalysis record in the Database, AnalysisResult (summary or detailed report), EmailNotification with results, AuditTrail record  
  
## 1.5 Permission Assignment Function   
Function ID: FR-05   
Description: Assign permissions to General Users based on predefined roles and permission types. The system must ensure the Administrator has the correct authority to assign permissions.   
Input: UserID, PermissionType, AllocationDate, ExpiryDate   
Output: PermissionAllocation record in the Database, AuditTrail record, Authentication system update, EmailNotification to user  
  
## 1.6 Permission Modification Function   
Function ID: FR-06   
Description: Modify existing permission assignments for General Users. The system must validate the modification request, update the Database, and synchronize with the Authentication System.   
Input: UserID, PermissionID, NewPermissionType, NewExpiryDate   
Output: Updated PermissionAllocation record in the Database, AuditTrail record, Authentication system update, EmailNotification to user  
  
## 1.7 General User Registration Function   
Function ID: FR-07   
Description: Allow Administrators to register new General Users by providing user details. The system must validate data integrity, check for duplicates, and send a confirmation email.   
Input: Name, Email, Role, JoinDate   
Output: GeneralUser record in the Database, Authentication system update, EmailNotification to user, AuditTrail record  
  
## 1.8 General User Deletion Function   
Function ID: FR-08   
Description: Allow Administrators to delete General User accounts. The system must confirm the deletion, update the Authentication System, and notify stakeholders via email.   
Input: UserID   
Output: Deleted GeneralUser record in the Database, Authentication system update, EmailNotification to Administrator, AuditTrail record  
  
## 1.9 General User Information Update Function   
Function ID: FR-09   
Description: Allow General Users or Administrators to update user information such as name, email, or role. The system must validate the update request and initiate approval workflows if necessary.   
Input: UserID, NewName, NewEmail, NewRole   
Output: Updated GeneralUser record in the Database, AuditTrail record, EmailNotification to user/Administrator, ApprovalWorkflow status update  
  
## 1.10 Administrator Role Management Function   
Function ID: FR-10   
Description: Allow Administrators to assign or modify administrator roles for users. The system must ensure that the Administrator has the necessary authority to perform the action.   
Input: AdminID, UserID, NewRole   
Output: Updated Admin record in the Database, AuditTrail record, Authentication system update, EmailNotification to Administrator, ApprovalWorkflow status update  
  
## 1.11 Approval Workflow Processing Function   
Function ID: FR-11   
Description: Process approval workflows initiated by users for asset or permission-related actions. The system must notify approvers, record the approval status, and update the related asset or permission records.   
Input: RequestID, ApprovalStatus (Approved/Rejected), ApproverID   
Output: Updated ApprovalWorkflow record in the Database, AuditTrail record, EmailNotification to requester/approvers, Updated Asset/PermissionAllocation record  
  
## 1.12 Approval Request Submission Function   
Function ID: FR-12   
Description: Allow users to submit approval requests for actions that require authorization. The system must validate the request and notify the required approvers.   
Input: UserID, AssetID or PermissionID, RequestDate, ApprovalReason   
Output: ApprovalRequest record in the Database, AuditTrail record, EmailNotification to approvers, ApprovalWorkflow status update  
  
## 1.13 Approval History Viewing Function   
Function ID: FR-13   
Description: Allow users to view the history of approval requests, including timestamps, approvers, and decisions. The system must ensure the user has permission to access this information.   
Input: RequestID, Filters (e.g., date range, approver)   
Output: ApprovalHistory records retrieved from the Database, AuditTrail record, Displayed ApprovalHistory on the system interface  
  
## 1.14 User Authentication Function   
Function ID: FR-14   
Description: Authenticate General Users or Administrators using login credentials. The system must validate the credentials, check user roles, and log the authentication event.   
Input: Username, Password   
Output: Authentication status (Success/Failure), AuthRecord in the Database, AuditTrail record, Session creation, Role-based redirection  
  
## 1.15 Email Notification Integration Function   
Function ID: FR-15   
Description: Configure and manage email notification settings for system events such as asset updates, approvals, and user actions. The system must support custom templates and recipient lists.   
Input: EventTriggers, RecipientList, EmailTemplate   
Output: EmailNotification record in the Database, Email sent via EmailSystem, AuditTrail record, ApprovalWorkflow status update  
  
## 1.16 Asset Data Import Function   
Function ID: FR-16   
Description: Allow Administrators to import asset data in formats such as CSV or Excel. The system must validate data integrity, map fields, and initiate approval workflows if required.   
Input: File (CSV/Excel), Mapping configuration   
Output: DataImportExportRecord in the Database, Updated Asset records, AuditTrail record, EmailNotification to Administrator, ApprovalWorkflow status update  
  
## 1.17 Asset Data Export Function   
Function ID: FR-17   
Description: Allow users to export asset data in formats such as CSV, Excel, or PDF. The system must validate export permissions, apply filters, and notify users of the export status.   
Input: Filters (e.g., category, status), ExportFormat   
Output: Exported file (CSV/Excel/PDF), DataImportExportRecord in the Database, AuditTrail record, EmailNotification to user/Administrator  
  
## 1.18 Audit Trail Viewing Function   
Function ID: FR-18   
Description: Allow General Users or Administrators to view audit trail records for system activities. The system must filter and display records while logging the access attempt.   
Input: Filters (e.g., date range, actor, action), UserID   
Output: Retrieved AuditTrail records, AuditTrail record for access, Displayed AuditTrail on system interface  
  
## 1.19 Asset Category Management Function   
Function ID: FR-19   
Description: Allow Administrators to manage asset categories, including adding, modifying, or deleting categories. The system must validate input and initiate approval workflows if required.   
Input: CategoryID, CategoryName, Description   
Output: Updated AssetCategory record in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.20 Asset Location Management Function   
Function ID: FR-20   
Description: Allow Administrators to manage asset locations, including building, room, and rack information. The system must validate location data and initiate approval workflows if required.   
Input: LocationID, Building, Room, Rack   
Output: Updated AssetLocation record in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.21 Usage Record Management Function   
Function ID: FR-21   
Description: Allow General Users or Administrators to manage usage records, including adding, modifying, or deleting records. The system must validate data and initiate approval workflows if required.   
Input: UsageRecordID, AssetID, UserID, UsageDate, Duration, Purpose   
Output: Updated UsageRecord in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.22 Permission Record Management Function   
Function ID: FR-22   
Description: Allow Administrators to manage permission records, including adding, modifying, or deleting records. The system must validate the permission changes and initiate approval workflows if required.   
Input: PermissionRecordID, UserID, PermissionID, AllocationDate, ExpiryDate   
Output: Updated PermissionRecord in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.23 Authentication Record Management Function   
Function ID: FR-23   
Description: Allow Administrators to manage authentication records, including adding, modifying, or deleting records. The system must validate the changes and initiate approval workflows if required.   
Input: AuthRecordID, UserID, AuthID, Timestamp, Status   
Output: Updated AuthenticationRecord in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update  
  
## 1.24 Email Notification Management Function   
Function ID: FR-24   
Description: Allow Administrators to manage email notification configurations, including event triggers, recipients, and templates. The system must validate configurations and synchronize with the Email System.   
Input: EmailNotificationID, EventTriggers, RecipientList, EmailTemplate   
Output: Updated EmailNotification record in the Database, EmailSystem configuration update, AuditTrail record, EmailNotification to Administrator  
  
## 1.25 Data Import/Export Record Management Function   
Function ID: FR-25   
Description: Allow Administrators to manage records of data import and export actions. The system must validate the input and initiate approval workflows if required.   
Input: ImportExportID, AssetID, UserID, Timestamp, Type (Import/Export), FilePath   
Output: Updated DataImportExportRecord in the Database, AuditTrail record, EmailNotification to stakeholders, ApprovalWorkflow status update

# External Description

# 2. External Interfaces  
  
This chapter defines and describes all external interfaces that the system interacts with, including user interfaces, hardware interfaces, software interfaces, and communication interfaces. These interfaces are essential for the system to function correctly and communicate with external entities.  
  
---  
  
## 2.1 User Interface  
  
The system interacts with users through a graphical user interface (GUI) that provides a clear and intuitive way to manage assets, permissions, and approval workflows. The GUI supports the following functionalities:  
  
- \*\*Asset Lifecycle Management (FR-01):\*\*   
 - Input: Users can update the lifecycle stage of an asset via a form.   
 - Output: The system displays the updated asset lifecycle information and provides feedback on the success or failure of the update.  
  
- \*\*Asset Usage Tracking (FR-02):\*\*   
 - Input: Users can log asset usage with a form specifying date, duration, and purpose.   
 - Output: The system displays a confirmation message and updates the usage record in the database.  
  
- \*\*Asset Report Generation (FR-03):\*\*   
 - Input: Users can select report types and apply filters through a GUI.   
 - Output: The system displays the generated report and provides options for downloading in CSV, Excel, or PDF formats.  
  
- \*\*Asset Data Analysis (FR-04):\*\*   
 - Input: Users can initiate analysis requests through the GUI.   
 - Output: The system displays analysis results and allows users to download detailed reports.  
  
- \*\*General User Registration (FR-07):\*\*   
 - Input: Administrators can input user details through a registration form.   
 - Output: The system provides a confirmation message and an email notification to the new user.  
  
- \*\*General User Deletion (FR-08):\*\*   
 - Input: Administrators can select a user and initiate deletion via a confirmation dialog.   
 - Output: The system displays a success/failure message and logs the deletion in the audit trail.  
  
- \*\*General User Information Update (FR-09):\*\*   
 - Input: Users or administrators can update user information via a form.   
 - Output: The system displays a confirmation message and logs the update in the audit trail.  
  
- \*\*Approval Request Submission (FR-12):\*\*   
 - Input: Users can submit approval requests through a form specifying the asset or permission request.   
 - Output: The system displays a confirmation and logs the submission in the approval workflow.  
  
- \*\*Approval History Viewing (FR-13):\*\*   
 - Input: Users can apply filters to view approval history.   
 - Output: The system displays the filtered approval history records.  
  
- \*\*User Authentication (FR-14):\*\*   
 - Input: Users can log in via a login form.   
 - Output: The system redirects the user to the appropriate interface based on their role and displays authentication status.  
  
- \*\*Asset Category Management (FR-19):\*\*   
 - Input: Administrators can add, modify, or delete asset categories through a dedicated interface.   
 - Output: The system displays a success/failure message and updates the category list accordingly.  
  
- \*\*Asset Location Management (FR-20):\*\*   
 - Input: Administrators can manage location details via a form.   
 - Output: The system displays confirmation and updates the location data.  
  
- \*\*Usage Record Management (FR-21):\*\*   
 - Input: Users or administrators can manage usage records via a form.   
 - Output: The system displays confirmation and updates the usage record.  
  
- \*\*Permission Record Management (FR-22):\*\*   
 - Input: Administrators can manage permission records via a form.   
 - Output: The system displays confirmation and updates the permission record.  
  
- \*\*Authentication Record Management (FR-23):\*\*   
 - Input: Administrators can manage authentication records via a form.   
 - Output: The system displays confirmation and updates the authentication record.  
  
- \*\*Email Notification Management (FR-24):\*\*   
 - Input: Administrators can configure email notification settings via a form.   
 - Output: The system displays confirmation and updates the email notification configuration.  
  
- \*\*Data Import/Export Record Management (FR-25):\*\*   
 - Input: Administrators can manage import/export records via a form.   
 - Output: The system displays confirmation and updates the import/export record.  
  
All user interface interactions are designed to be intuitive and user-friendly, with appropriate feedback and confirmation messages to ensure clarity and usability.  
  
---  
  
## 2.2 Hardware Interface  
  
The system does not require direct interaction with specific hardware devices. However, it may be deployed on servers or cloud infrastructure that requires compatibility with standard hardware components such as:  
  
- \*\*Servers:\*\* The system may be hosted on physical or virtual servers, which must support the required operating system, CPU, memory, and storage specifications.  
- \*\*Storage Devices:\*\* The system may interact with external storage systems for backups or data persistence, requiring standard storage protocols such as NFS, SMB, or cloud storage APIs (e.g., Amazon S3, Azure Blob Storage).  
- \*\*Input/Output Devices:\*\* Users may interact with the system via standard input devices (e.g., keyboards, mice) and output devices (e.g., monitors, printers), especially when generating and printing reports or downloading files.  
  
No specific hardware communication protocols are required beyond standard network and storage interfaces. The system is designed to be agnostic to the underlying hardware as long as the required software and network interfaces are available.  
  
---  
  
## 2.3 Software Interface  
  
The system interacts with various software components and external systems to manage asset data, permissions, and workflows. These software interfaces include:  
  
- \*\*Database (DB):\*\*   
 - \*\*Description:\*\* The system interacts with a relational database to store and retrieve asset, user, permission, and audit data.   
 - \*\*Interaction Method:\*\* SQL queries or an ORM (Object-Relational Mapping) tool are used to manage database records.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* Asset and user data, permission assignments, approval workflow status, and configuration settings.   
 - \*\*Output:\*\* Records are updated, inserted, or deleted in the database (e.g., AssetLifeCycle, AssetUsage, PermissionAllocation, ApprovalWorkflow, AuditTrail).  
  
- \*\*Email System (ES):\*\*   
 - \*\*Description:\*\* The system sends and receives email notifications for events such as asset updates, approval requests, and user actions.   
 - \*\*Interaction Method:\*\* SMTP (Simple Mail Transfer Protocol) or an email service API (e.g., SendGrid, Amazon SES) is used to send emails.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* Email templates, recipient lists, and event triggers (e.g., system-generated emails for notifications).   
 - \*\*Output:\*\* Email notifications are sent to stakeholders, users, or administrators.  
  
- \*\*Authentication System (AS):\*\*   
 - \*\*Description:\*\* The system synchronizes with an external authentication system to validate user credentials and manage user roles.   
 - \*\*Interaction Method:\*\* REST API or LDAP (Lightweight Directory Access Protocol) is used to interact with the authentication system.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* User credentials, role assignments, and permission changes.   
 - \*\*Output:\*\* Authentication system is updated with new user records, role assignments, or permission modifications.  
  
- \*\*Data Import/Export System (I/ES):\*\*   
 - \*\*Description:\*\* The system supports importing and exporting data in formats such as CSV, Excel, and PDF.   
 - \*\*Interaction Method:\*\* The system reads and writes data from/to files using standard file I/O operations or libraries (e.g., pandas for CSV/Excel).   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* File (CSV/Excel), mapping configuration, and filters.   
 - \*\*Output:\*\* Data is imported into the database or exported to a file, and a record is stored in the DataImportExportRecord table.  
  
- \*\*Report Generation Tools:\*\*   
 - \*\*Description:\*\* The system generates reports in CSV, Excel, and PDF formats.   
 - \*\*Interaction Method:\*\* Libraries or tools such as Python's pandas (for CSV/Excel) and ReportLab or PDFKit (for PDF) are used to create and format reports.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* Report type, filters, and user preferences.   
 - \*\*Output:\*\* Report file in the requested format is generated and delivered to the user.  
  
All software interfaces are designed to ensure seamless integration with external systems and to support the required functionalities as defined in the functional requirements.  
  
---  
  
## 2.4 Communication Interface  
  
The system communicates with external entities through various communication protocols and mechanisms, including:  
  
- \*\*Email Notifications (FR-15, FR-24):\*\*   
 - \*\*Description:\*\* Email notifications are sent to users and stakeholders for system events such as asset lifecycle updates, approval requests, and user actions.   
 - \*\*Interaction Method:\*\* SMTP or email service APIs are used to send notifications.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* Email content, recipient list, and event trigger details.   
 - \*\*Output:\*\* Email is delivered to the recipient, and the system logs the event in the audit trail.  
  
- \*\*Approval Workflow Communication (FR-11, FR-12, FR-13):\*\*   
 - \*\*Description:\*\* The system communicates approval status updates to requesters and approvers.   
 - \*\*Interaction Method:\*\* Internal messaging or email notifications are used to inform users of their approval status.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* Approval status (Approved/Rejected), approver ID, and request ID.   
 - \*\*Output:\*\* Approval status is updated in the system, and users are notified via email or in-system messages.  
  
- \*\*Web Browsing (FR-14, FR-16, FR-17, FR-18, FR-19, FR-20, FR-21, FR-22, FR-23, FR-25):\*\*   
 - \*\*Description:\*\* Users access the system via a web browser, and the system communicates with the user's browser through HTTP/HTTPS protocols.   
 - \*\*Interaction Method:\*\* The system uses a web framework (e.g., Flask, Django) to serve dynamic content and process user requests.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* HTTP requests from the user's browser, including form submissions, filters, and file uploads.   
 - \*\*Output:\*\* HTTP responses with HTML, JSON, or file downloads (e.g., CSV, Excel, PDF).  
  
- \*\*API Communication (FR-05, FR-06, FR-10, FR-11, FR-12, FR-22, FR-23, FR-25):\*\*   
 - \*\*Description:\*\* The system may interact with external APIs for user management, authentication, and audit trail logging.   
 - \*\*Interaction Method:\*\* RESTful APIs or GraphQL endpoints are used to exchange data.   
 - \*\*Inputs/Outputs:\*\*   
 - \*\*Input:\*\* API requests with parameters such as UserID, PermissionID, AllocationDate, etc.   
 - \*\*Output:\*\* API responses confirming the success or failure of an action, along with any updated data.  
  
All communication interfaces are designed to ensure secure, reliable, and efficient data exchange between the system and external entities.  
  
---  
  
## 2.5 Summary of External Data Sources  
  
To ensure consistency with the functional requirements, the following external data sources are defined in this section:  
  
- \*\*AssetLifeCycle Record (FR-01):\*\* Stored in the database and updated during asset lifecycle changes.  
- \*\*AssetUsage Record (FR-02, FR-21):\*\* Stored in the database and updated when users log asset usage.  
- \*\*PermissionAllocation Record (FR-05, FR-06, FR-22):\*\* Stored in the database and synchronized with the authentication system.  
- \*\*GeneralUser Record (FR-07, FR-08, FR-09):\*\* Stored in the database and managed via the authentication system.  
- \*\*ApprovalWorkflow Record (FR-11, FR-12, FR-13):\*\* Stored in the database and updated with status changes.  
- \*\*Authentication Record (FR-14, FR-23):\*\* Stored in the authentication system and database for tracking login events.  
- \*\*EmailNotification Record (FR-15, FR-24):\*\* Stored in the database and sent via the email system.  
- \*\*DataImportExportRecord (FR-16, FR-17, FR-25):\*\* Stored in the database for tracking import/export actions.  
- \*\*AuditTrail Record (All FRs):\*\* Stored in the database to log all system activities and access attempts.  
  
Each of these data sources is directly referenced in the functional requirements and is clearly defined in the corresponding software or communication interfaces.  
  
---  
  
This concludes the External Interfaces chapter of the Software Requirements Specification. Each interface has been classified and described in detail to ensure clarity and ease of implementation. Developers can refer to this section to understand how the system interacts with external entities and to ensure proper integration during development.

# Use Case

Use Case Name: Asset Lifecycle Management   
Use Case ID: UC-01   
Actors: General User, Administrator, Approval Workflow, Authentication System, Email System, Database, Audit Trail   
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database for storing and retrieving asset-related data.   
3. The Approval Workflow is configured and active.   
4. The Email System is operational to send notifications.   
5. An asset must exist in the system or be newly created.   
  
Postconditions:   
1. The asset lifecycle is updated in the Database.   
2. Notifications are sent via the Email System to relevant stakeholders.   
3. An Audit Trail is created to log all changes to the asset lifecycle.   
4. The Approval Workflow is completed if required.   
  
Main Flow:   
1. The General User or Administrator accesses the Asset Lifecycle Management feature.   
2. The system displays the list of assets or a form for creating a new asset.   
3. The user selects an asset or creates a new one.   
4. The user chooses a lifecycle action (e.g., acquisition, deployment, maintenance, decommissioning).   
5. The system validates the action and the user's permissions.   
6. The system initiates the Approval Workflow if the action requires approval.   
7. The Approval Workflow is completed by authorized users.   
8. The system updates the asset's lifecycle status in the Database.   
9. The system logs the change in the Audit Trail.   
10. The system sends a confirmation email to the user and relevant stakeholders.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to perform the lifecycle action, the system denies the request and logs the attempt in the Audit Trail.   
2. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
3. If the Approval Workflow is rejected, the system cancels the lifecycle action and logs the rejection in the Audit Trail.   
4. If the Email System is not operational, the system logs an error and notifies the Administrator.   
5. If the Database is unavailable, the system displays an error message and aborts the lifecycle action.  
  
Use Case Name: Asset Usage Tracking   
Use Case ID: UC-02   
Actors: General User, Administrator, Approval Workflow, Authentication System, Email System, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database for storing and retrieving asset usage data.   
3. The Approval Workflow is configured and active if required.   
4. The Email System is operational to send notifications.   
5. An asset must exist in the system and be associated with usage records.   
  
Postconditions:   
1. The asset usage record is updated in the Database.   
2. Notifications are sent via the Email System to relevant stakeholders if necessary.   
3. An Audit Trail is created to log all changes to the asset usage.   
4. The Approval Workflow is completed if required.   
  
Main Flow:   
1. The General User or Administrator accesses the Asset Usage Tracking feature.   
2. The system displays the asset usage history or a form to record new usage.   
3. The user selects an asset for which usage needs to be tracked.   
4. The user inputs the usage details (e.g., usage time, activity, location, user involved).   
5. The system validates the input data and the user's permissions.   
6. If the usage requires approval, the system initiates the Approval Workflow.   
7. The Approval Workflow is completed by authorized users.   
8. The system stores the usage data in the Database.   
9. The system logs the usage tracking in the Audit Trail.   
10. The system sends a confirmation email to the user and relevant stakeholders.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to track usage for the selected asset, the system denies the request and logs the attempt in the Audit Trail.   
2. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
3. If the Approval Workflow is rejected, the system cancels the usage tracking and logs the rejection in the Audit Trail.   
4. If the Email System is not operational, the system logs an error and notifies the Administrator.   
5. If the Database is unavailable, the system displays an error message and aborts the usage tracking.  
  
Use Case Name: Generate Asset Reports   
Use Case ID: UC-03   
Actors: General User, Administrator, Email System, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to retrieve asset-related data.   
3. The Email System is operational if email notifications are needed.   
4. The user has the necessary permissions to generate reports.   
5. At least one asset exists in the system with available usage and lifecycle data.   
  
Postconditions:   
1. The generated report is saved in the Database or made available for download.   
2. Notifications are sent via the Email System to the user and stakeholders if requested.   
3. An Audit Trail is created to log the report generation activity.   
4. The system confirms the successful generation of the report.   
  
Main Flow:   
1. The General User or Administrator navigates to the "Generate Asset Reports" feature.   
2. The system displays available report types (e.g., asset lifecycle report, asset usage report, summary report).   
3. The user selects a report type and specifies any filters (e.g., time range, asset category).   
4. The system validates the report request and the user's permissions.   
5. The system retrieves the relevant data from the Database.   
6. The system generates the report based on the selected parameters.   
7. The system offers the option to download the report or send it via email.   
8. If requested, the system sends the report via the Email System.   
9. The system logs the report generation in the Audit Trail.   
10. The system confirms the completion of the report generation.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to generate the report, the system denies the request and logs the attempt in the Audit Trail.   
2. If the Database is unavailable, the system displays an error message and aborts the report generation.   
3. If the Email System is not operational and the user requested email delivery, the system logs an error and notifies the Administrator.   
4. If no assets match the specified filters, the system generates a report with a message indicating no data found.   
5. If the report generation process encounters an error, the system displays an error message and logs the event in the Audit Trail.  
  
Use Case Name: Analyze Asset Data   
Use Case ID: UC-04   
Actors: General User, Administrator, Approval Workflow, Authentication System, Email System, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database for retrieving and analyzing asset data.   
3. The Approval Workflow is configured and active if analysis requires approval.   
4. The Email System is operational to send notifications if required.   
5. At least one asset record exists in the system with available data for analysis.   
  
Postconditions:   
1. The asset data analysis results are stored in the Database or made available for viewing.   
2. Notifications are sent via the Email System to the user and stakeholders if requested.   
3. An Audit Trail is created to log the analysis activity and any changes.   
4. The Approval Workflow is completed if initiated.   
5. The system confirms the completion of the analysis.   
  
Main Flow:   
1. The General User or Administrator accesses the "Analyze Asset Data" feature.   
2. The system displays available analysis options (e.g., performance analysis, usage trends, lifecycle efficiency).   
3. The user selects an asset and chooses an analysis type.   
4. The system validates the user's permissions and the selected asset.   
5. If approval is required for the analysis, the system initiates the Approval Workflow.   
6. The Approval Workflow is completed by authorized users.   
7. The system retrieves the relevant asset data from the Database.   
8. The system performs the analysis and generates a summary or detailed report.   
9. The system displays the analysis results to the user or provides a download option.   
10. If requested, the system sends the analysis results via the Email System.   
11. The system logs the analysis in the Audit Trail.   
12. The system confirms the completion of the analysis.   
13. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to analyze the asset data, the system denies the request and logs the attempt in the Audit Trail.   
2. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
3. If the Approval Workflow is rejected, the analysis is canceled, and the system logs the rejection in the Audit Trail.   
4. If the Email System is not operational and the user requested email delivery, the system logs an error and notifies the Administrator.   
5. If the Database is unavailable, the system displays an error message and aborts the analysis.   
6. If the asset data is incomplete or corrupted, the system alerts the user and logs the issue in the Audit Trail.  
  
Use Case Name: Assign Permissions   
Use Case ID: UC-05   
Actors: Administrator, Authentication System, Database, Audit Trail   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve permission-related data.   
3. The Authentication System is operational to validate user credentials.   
4. At least one user account exists in the system.   
5. Permission levels and roles are predefined in the system.   
  
Postconditions:   
1. The user's permissions are updated in the Database.   
2. An Audit Trail is created to log the permission assignment.   
3. The system confirms the successful assignment of permissions.   
4. If applicable, the Authentication System is updated with the new permissions.   
  
Main Flow:   
1. The Administrator accesses the "Assign Permissions" feature.   
2. The system displays a list of user accounts and available permission roles.   
3. The Administrator selects a user and assigns one or more roles.   
4. The system validates the selected roles and the Administrator's authority.   
5. The system updates the user's permissions in the Database.   
6. The system logs the permission assignment in the Audit Trail.   
7. The system sends a confirmation message to the Administrator.   
8. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have authority to assign the selected roles, the system denies the request and logs the attempt in the Audit Trail.   
2. If the selected user does not exist, the system displays an error message and aborts the permission assignment.   
3. If the Database is unavailable, the system displays an error message and aborts the process.   
4. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.   
5. If the system encounters an error during permission assignment, it displays an error message and logs the event in the Audit Trail.  
  
Use Case Name: Modify Permissions   
Use Case ID: UC-06   
Actors: Administrator, Authentication System, Database, Audit Trail   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve permission-related data.   
3. The Authentication System is operational to validate user credentials and manage permissions.   
4. The user whose permissions are to be modified must exist in the system.   
5. Permission levels and roles are predefined in the system.   
  
Postconditions:   
1. The user's permissions are updated in the Database.   
2. The Authentication System is updated with the new permissions.   
3. An Audit Trail is created to log the permission modification.   
4. The system confirms the successful modification of permissions.   
  
Main Flow:   
1. The Administrator accesses the "Modify Permissions" feature.   
2. The system displays a list of users and their current permission roles.   
3. The Administrator selects a user and modifies one or more roles.   
4. The system validates the changes and the Administrator's authority.   
5. The system updates the user's permissions in the Database.   
6. The system updates the Authentication System with the new permission settings.   
7. The system logs the permission modification in the Audit Trail.   
8. The system sends a confirmation message to the Administrator.   
9. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have authority to modify the selected roles, the system denies the request and logs the attempt in the Audit Trail.   
2. If the selected user does not exist, the system displays an error message and aborts the permission modification.   
3. If the Database is unavailable, the system displays an error message and aborts the process.   
4. If the Authentication System fails to update the permissions, the system logs an error and notifies the Administrator.   
5. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Register General User   
Use Case ID: UC-07   
Actors: Administrator, Authentication System, Email System, Database, Audit Trail   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database for storing user account information.   
3. The Authentication System is operational to validate user credentials and create new accounts.   
4. The Email System is functional to send confirmation and notification emails.   
5. The system allows registration of new General Users.   
  
Postconditions:   
1. A new General User account is created in the Database.   
2. A confirmation email is sent to the General User via the Email System.   
3. The registration event is logged in the Audit Trail.   
4. The Authentication System is updated with the new user's credentials.   
5. The Administrator receives a confirmation message of successful registration.   
  
Main Flow:   
1. The Administrator accesses the "Register General User" feature.   
2. The system displays a form for entering the new user's details (e.g., name, email, role).   
3. The Administrator fills in the required information and submits the form.   
4. The system validates the input data and checks for duplicate entries.   
5. The system creates the new General User account in the Database.   
6. The system updates the Authentication System with the new user’s credentials.   
7. The system sends a confirmation email to the new user’s email address.   
8. The system logs the registration in the Audit Trail.   
9. The system provides a confirmation message to the Administrator.   
10. The use case is completed.   
  
Alternative Flow:   
1. If the input data is invalid or incomplete, the system displays an error message and aborts the registration.   
2. If a user with the same email already exists, the system displays a duplicate entry error and stops the process.   
3. If the Database is unavailable, the system displays an error message and aborts the registration.   
4. If the Email System fails to send the confirmation email, the system logs the error and notifies the Administrator.   
5. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Delete General User   
Use Case ID: UC-08   
Actors: Administrator, Authentication System, Email System, Database, Audit Trail   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to retrieve and delete user account information.   
3. The Authentication System is operational to validate user credentials and manage account deletion.   
4. The Email System is functional to send notification emails.   
5. The user account to be deleted must exist in the system.   
  
Postconditions:   
1. The General User account is deleted from the Database.   
2. The Authentication System is updated to remove the deleted user's credentials.   
3. A notification email is sent to the Administrator and possibly other stakeholders via the Email System.   
4. The deletion event is logged in the Audit Trail.   
5. The system confirms the successful deletion of the user account.   
  
Main Flow:   
1. The Administrator accesses the "Delete General User" feature.   
2. The system displays a list of existing General User accounts.   
3. The Administrator selects a user account for deletion.   
4. The system validates the Administrator's authority to delete the selected user.   
5. The system confirms the deletion request with the Administrator.   
6. The system proceeds to delete the selected user account from the Database.   
7. The Authentication System is updated to remove the deleted user's access credentials.   
8. The system logs the deletion event in the Audit Trail.   
9. The system sends a confirmation email to the Administrator.   
10. The system confirms the completion of the deletion process.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have authority to delete the selected user, the system denies the request and logs the attempt in the Audit Trail.   
2. If the selected user account does not exist, the system displays an error message and aborts the deletion process.   
3. If the Database is unavailable, the system displays an error message and aborts the deletion.   
4. If the Email System fails to send the confirmation email, the system logs the error and notifies the Administrator.   
5. If the Audit Trail fails to record the deletion event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Update General User Information   
Use Case ID: UC-09   
Actors: General User, Administrator, Authentication System, Email System, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database for storing and retrieving user account information.   
3. The Authentication System is operational to validate user credentials and update account details.   
4. The Email System is functional to send confirmation and notification emails.   
5. The user account to be updated must exist in the system.   
  
Postconditions:   
1. The General User's information is updated in the Database.   
2. The Authentication System is updated with the new information if applicable (e.g., password or email changes).   
3. A confirmation email is sent to the affected user and possibly to the Administrator.   
4. The update event is logged in the Audit Trail.   
5. The system confirms the successful update of the user's information.   
  
Main Flow:   
1. The General User or Administrator navigates to the "Update General User Information" feature.   
2. The system displays the user's current information (e.g., name, email, role, contact details).   
3. The user modifies the desired fields and submits the update request.   
4. The system validates the input data and the user's authority to perform the update.   
5. If the update involves sensitive information (e.g., password, role), the system may initiate the Approval Workflow.   
6. The Approval Workflow is completed by authorized users if required.   
7. The system updates the user's information in the Database.   
8. The system updates the Authentication System if changes affect login credentials.   
9. The system logs the update in the Audit Trail.   
10. The system sends a confirmation email to the user and possibly to the Administrator.   
11. The system confirms the completion of the update.   
12. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have authority to update the information, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the update.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the update and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the update.   
6. If the Email System fails to send the confirmation email, the system logs the error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage Administrator Roles   
Use Case ID: UC-10   
Actors: Administrator, Authentication System, Database, Audit Trail   
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve administrator role information.   
3. The Authentication System is operational to validate user credentials and manage role assignments.   
4. Administrator roles and their associated permissions are predefined in the system.   
5. At least one user account exists in the system.   
  
Postconditions:   
1. The administrator roles are updated in the Database.   
2. The Authentication System is updated with the new role assignments.   
3. An Audit Trail is created to log the role management activity.   
4. The system confirms the successful management of administrator roles.   
  
Main Flow:   
1. The Administrator accesses the "Manage Administrator Roles" feature.   
2. The system displays a list of users and available administrator roles.   
3. The Administrator selects a user and assigns or modifies their administrator role.   
4. The system validates the selected role and the Administrator's authority to make changes.   
5. The system updates the user's administrator role in the Database.   
6. The system updates the Authentication System with the new role permissions.   
7. The system logs the role management in the Audit Trail.   
8. The system provides a confirmation message to the Administrator.   
9. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have authority to assign or modify the selected roles, the system denies the request and logs the attempt in the Audit Trail.   
2. If the selected user does not exist, the system displays an error message and aborts the role management.   
3. If the Database is unavailable, the system displays an error message and aborts the process.   
4. If the Authentication System fails to update the role, the system logs an error and notifies the Administrator.   
5. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Process Approval   
Use Case ID: UC-11   
Actors: General User, Administrator, Approval Workflow, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to retrieve and store approval-related data.   
3. The Approval Workflow is configured and active for the relevant process.   
4. The Audit Trail is operational to record approval events.   
5. A request must exist in the system that requires approval.   
  
Postconditions:   
1. The approval status of the request is updated in the Database.   
2. The approval event is logged in the Audit Trail.   
3. The Approval Workflow is either completed or pending based on the action.   
4. The system confirms the approval process outcome.   
  
Main Flow:   
1. The General User or Administrator initiates a request that requires approval.   
2. The system triggers the Approval Workflow and identifies the required approvers.   
3. The system sends a notification to the approvers, requesting their approval.   
4. The approvers review the request and either approve or reject it.   
5. The system updates the approval status in the Database based on the decision.   
6. The system logs the approval action in the Audit Trail.   
7. The system confirms the approval process outcome to the requester and relevant stakeholders.   
8. The use case is completed.   
  
Alternative Flow:   
1. If the approver does not have authority to approve the request, the system denies the action and logs the attempt in the Audit Trail.   
2. If no approvers are assigned to the workflow, the system displays an error and aborts the process.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the request and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the approval process.   
6. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Submit Approval Request   
Use Case ID: UC-12   
Actors: General User, Administrator, Approval Workflow, Email System, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve approval request data.   
3. The Approval Workflow is configured and active for the relevant process.   
4. The Email System is operational to send notifications to approvers.   
5. A valid asset or user-related action must exist that requires an approval request.   
  
Postconditions:   
1. The approval request is recorded in the Database.   
2. The Approval Workflow is triggered with the appropriate approvers notified.   
3. The approval request is logged in the Audit Trail.   
4. The system confirms the submission of the approval request.   
  
Main Flow:   
1. The General User or Administrator initiates an action that requires approval (e.g., asset modification, permission assignment).   
2. The system displays a form for submitting the approval request, including the reason and details of the action.   
3. The user fills in the form and submits the approval request.   
4. The system validates the input data and checks if the action indeed requires approval.   
5. The system records the approval request in the Database.   
6. The system triggers the Approval Workflow and identifies the required approvers.   
7. The system sends a notification email to the approvers via the Email System.   
8. The system logs the submission of the approval request in the Audit Trail.   
9. The system confirms the successful submission to the user.   
10. The use case is completed.   
  
Alternative Flow:   
1. If the action does not require approval, the system skips the approval process and proceeds with the action directly.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the submission.   
3. If the Approval Workflow is not configured for the action, the system displays an error and aborts the process.   
4. If the Email System is not operational, the system logs an error and notifies the Administrator.   
5. If the Database is unavailable, the system displays an error message and aborts the submission.   
6. If the user does not have permission to submit the approval request, the system denies the request and logs the attempt in the Audit Trail.  
  
Use Case Name: View Approval History   
Use Case ID: UC-13   
Actors: General User, Administrator, Approval Workflow, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to retrieve approval-related data.   
3. The Approval Workflow is configured and active.   
4. At least one approval request must exist in the system with a recorded history.   
5. The user has the necessary permissions to view approval history.   
  
Postconditions:   
1. The approval history is displayed to the user.   
2. The system logs the access to the approval history in the Audit Trail.   
3. The system confirms the successful retrieval of the approval history.   
4. No changes are made to the approval data or the asset.   
  
Main Flow:   
1. The General User or Administrator navigates to the "View Approval History" feature.   
2. The system displays a list of approval requests or a search interface.   
3. The user selects an approval request to view its history.   
4. The system retrieves the approval history from the Database.   
5. The system presents the approval history to the user, including timestamps, approvers, and decisions.   
6. The system logs the viewing action in the Audit Trail.   
7. The system confirms the retrieval of the approval history to the user.   
8. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to view the approval history, the system denies the request and logs the attempt in the Audit Trail.   
2. If the selected approval request does not exist, the system displays an error message and aborts the process.   
3. If the Database is unavailable, the system displays an error message and aborts the retrieval.   
4. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.   
5. If the approval history contains no data, the system displays a message indicating no history found.  
  
Use Case Name: Implement Authentication   
Use Case ID: UC-14   
Actors: General User, Administrator, Authentication System, Database, Audit Trail   
Preconditions:   
1. The Authentication System is operational and properly configured.   
2. The system has access to the Database to store and retrieve user authentication data.   
3. The user (General User or Administrator) must provide valid login credentials.   
4. The Audit Trail is available to log authentication-related activities.   
5. The system has predefined roles and permissions for user authentication.   
  
Postconditions:   
1. The user is authenticated and granted access to the system based on their role.   
2. The authentication event is logged in the Audit Trail.   
3. The Authentication System is updated with the login session information.   
4. The system confirms the successful authentication.   
5. The user is redirected to the appropriate interface based on their role.   
  
Main Flow:   
1. The user accesses the login interface of the system.   
2. The user enters their username and password.   
3. The system validates the credentials against the Database.   
4. The system checks the user's role and permissions in the Authentication System.   
5. If the credentials are valid and the user has the necessary permissions, the system authenticates the user.   
6. The system logs the successful authentication in the Audit Trail.   
7. The system establishes a login session for the user.   
8. The user is redirected to their respective dashboard.   
9. The use case is completed.   
  
Alternative Flow:   
1. If the user enters invalid credentials, the system denies access and logs the failed attempt in the Audit Trail.   
2. If the user account is locked or disabled, the system displays an error and logs the event in the Audit Trail.   
3. If the Database is unavailable, the system displays an error message and aborts the authentication process.   
4. If the Authentication System fails to validate the user, the system logs the error and notifies the Administrator.   
5. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Integrate Email Notifications   
Use Case ID: UC-15   
Actors: Administrator, Email System, Database, Audit Trail   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve email notification configurations.   
3. The Email System is operational and properly configured.   
4. The Audit Trail is available to log email integration activities.   
5. The system allows customization of email templates and notification settings.   
  
Postconditions:   
1. Email notification configurations are updated in the Database.   
2. The Email System is configured to send notifications as specified.   
3. The integration event is logged in the Audit Trail.   
4. The system confirms the successful integration of email notifications.   
5. Email templates and notification triggers are set for relevant system events.   
  
Main Flow:   
1. The Administrator accesses the "Integrate Email Notifications" feature.   
2. The system displays a configuration interface for email notification settings.   
3. The Administrator selects the system events that should trigger email notifications (e.g., asset updates, approval requests).   
4. The Administrator configures the email templates for each selected event.   
5. The system validates the configuration and ensures the Email System is connected.   
6. The system stores the email notification settings in the Database.   
7. The system logs the configuration in the Audit Trail.   
8. The system confirms the successful integration of email notifications.   
9. The use case is completed.   
  
Alternative Flow:   
1. If the selected system events are invalid or not supported, the system displays an error message and aborts the integration.   
2. If the Email System is not properly configured, the system logs an error and notifies the Administrator.   
3. If the Database is unavailable, the system displays an error message and aborts the process.   
4. If the Administrator does not have permission to configure email notifications, the system denies the request and logs the attempt in the Audit Trail.   
5. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Import Asset Data   
Use Case ID: UC-16   
Actors: Administrator, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store imported asset data.   
3. The Audit Trail is operational to record data import activities.   
4. The Approval Workflow is configured for asset data import if required.   
5. The Email System is functional to send confirmation or notification emails.   
6. A valid data file (e.g., CSV, Excel) is prepared for import.   
  
Postconditions:   
1. The asset data is imported and stored in the Database.   
2. The import event is logged in the Audit Trail.   
3. A confirmation email is sent to the Administrator and possibly stakeholders.   
4. The Approval Workflow is completed if initiated.   
5. The system confirms the successful import of asset data.   
  
Main Flow:   
1. The Administrator navigates to the "Import Asset Data" feature.   
2. The system displays an interface for uploading the asset data file and selecting the import configuration.   
3. The Administrator uploads the file and selects mapping fields for the import.   
4. The system validates the file format, data integrity, and mapping configuration.   
5. If the import requires approval, the system initiates the Approval Workflow.   
6. The Approval Workflow is completed by authorized users.   
7. The system processes the file and imports the asset data into the Database.   
8. The system logs the import in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and stakeholders.   
10. The system displays a success message and the use case is completed.   
  
Alternative Flow:   
1. If the file format is invalid, the system displays an error and aborts the import.   
2. If the data mapping is incorrect, the system alerts the Administrator and stops the process.   
3. If the Administrator does not have permission to import data, the system denies the request and logs the attempt in the Audit Trail.   
4. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder to the approvers.   
5. If the Approval Workflow is rejected, the system cancels the import and logs the rejection in the Audit Trail.   
6. If the Database is unavailable, the system displays an error and aborts the import.   
7. If the Email System fails to send the confirmation email, the system logs the error and notifies the Administrator.   
8. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Export Asset Data   
Use Case ID: UC-17   
Actors: General User, Administrator, Email System, Database, Audit Trail   
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to retrieve asset data.   
3. The Email System is operational for sending export confirmation emails.   
4. The Audit Trail is available to log export-related activities.   
5. The user has the necessary permissions to export asset data.   
6. The system supports export formats such as CSV, Excel, or PDF.   
  
Postconditions:   
1. The asset data is exported in the requested format.   
2. The export event is logged in the Audit Trail.   
3. A confirmation email is sent to the user and possibly stakeholders.   
4. The exported data is made available for download or sent via email.   
5. The system confirms the successful completion of the export.   
  
Main Flow:   
1. The General User or Administrator accesses the "Export Asset Data" feature.   
2. The system displays available export formats and options (e.g., export all assets, filter by category or status).   
3. The user selects the export format and applies any filters.   
4. The system validates the export request and the user's permissions.   
5. The system retrieves the relevant asset data from the Database.   
6. The system generates the export file in the selected format.   
7. The system offers the option to download the file or send it via email.   
8. If requested, the system sends the file via the Email System.   
9. The system logs the export action in the Audit Trail.   
10. The system confirms the export completion to the user.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to export data, the system denies the request and logs the attempt in the Audit Trail.   
2. If the Database is unavailable, the system displays an error and aborts the export.   
3. If the Email System is not operational and the user requested email delivery, the system logs an error and notifies the Administrator.   
4. If the export file generation encounters an error, the system displays an error message and logs the event in the Audit Trail.   
5. If no assets match the selected filters, the system generates a file with a message indicating no data found.   
6. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: View Audit Trail   
Use Case ID: UC-18   
Actors: General User, Administrator, Database, Audit Trail   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to retrieve audit trail data.   
3. The Audit Trail is enabled and contains records of system activities.   
4. The user has the necessary permissions to view the audit trail.   
5. The system interface for viewing the audit trail is accessible.   
  
Postconditions:   
1. The audit trail records are displayed to the user.   
2. The viewing action is logged in the Audit Trail.   
3. No changes are made to the audit trail data.   
4. The system confirms the successful retrieval of the audit trail.   
  
Main Flow:   
1. The General User or Administrator navigates to the "View Audit Trail" feature.   
2. The system displays a search or filter interface for the audit trail entries.   
3. The user selects specific filters (e.g., date range, actor, action type).   
4. The system retrieves the relevant audit trail records from the Database.   
5. The system presents the audit trail entries to the user, including timestamps, actions, and involved actors.   
6. The system logs the viewing action in the Audit Trail.   
7. The system confirms the retrieval of the audit trail to the user.   
8. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to view the audit trail, the system denies the request and logs the attempt in the Audit Trail.   
2. If the selected filters return no audit trail records, the system displays a message indicating no data found.   
3. If the Database is unavailable, the system displays an error message and aborts the retrieval.   
4. If the Audit Trail fails to record the viewing event, the system logs an error and notifies the Administrator.   
5. If the system interface for viewing the audit trail is inaccessible, the system displays an error and stops the process.  
  
Use Case Name: Manage Asset Category   
Use Case ID: UC-19   
Actors: Administrator, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database for storing and retrieving asset category information.   
3. The Audit Trail is enabled to record asset category management activities.   
4. The Approval Workflow is configured and active if category changes require approval.   
5. The Email System is functional to send notifications related to category changes.   
6. At least one asset category must exist in the system, or the Administrator is ready to create a new one.   
  
Postconditions:   
1. The asset category is added, modified, or deleted in the Database.   
2. The change to the asset category is logged in the Audit Trail.   
3. The Approval Workflow is completed if initiated.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the asset category management action.   
  
Main Flow:   
1. The Administrator accesses the "Manage Asset Category" feature.   
2. The system displays a list of existing asset categories and provides options to add, modify, or delete categories.   
3. The Administrator selects an action (add, modify, or delete) and provides the necessary details.   
4. The system validates the input data and the Administrator's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted asset category.   
8. The system logs the asset category management action in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and possibly stakeholders.   
10. The system confirms the completion of the asset category management action.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have permission to manage asset categories, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the asset category change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and email notification is requested, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage Asset Location   
Use Case ID: UC-20   
Actors: Administrator, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve asset location information.   
3. The Audit Trail is enabled to record asset location management activities.   
4. The Approval Workflow is configured and active if location changes require approval.   
5. The Email System is functional to send notifications related to location changes.   
6. At least one asset must exist in the system for location management.   
  
Postconditions:   
1. The asset location is added, modified, or deleted in the Database.   
2. The change to the asset location is logged in the Audit Trail.   
3. The Approval Workflow is completed if initiated.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the asset location management action.   
  
Main Flow:   
1. The Administrator accesses the "Manage Asset Location" feature.   
2. The system displays a list of existing asset locations and provides options to add, modify, or delete locations.   
3. The Administrator selects an action (add, modify, or delete) and provides the necessary details for the asset location.   
4. The system validates the input data and the Administrator's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted asset location.   
8. The system logs the asset location management action in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and possibly stakeholders.   
10. The system confirms the completion of the asset location management action.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have permission to manage asset locations, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the asset location change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and email notification is requested, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage Usage Record   
Use Case ID: UC-21   
Actors: General User, Administrator, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The General User or Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve usage record data.   
3. The Audit Trail is enabled and available to log changes to usage records.   
4. The Approval Workflow is configured and active if managing usage records requires approval.   
5. The Email System is operational to send notifications if required.   
6. At least one usage record must exist in the system, or the user is ready to create a new one.   
  
Postconditions:   
1. The usage record is added, modified, or deleted in the Database.   
2. The change to the usage record is logged in the Audit Trail.   
3. The Approval Workflow is completed if initiated.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the usage record management action.   
  
Main Flow:   
1. The General User or Administrator navigates to the "Manage Usage Record" feature.   
2. The system displays a list of existing usage records and provides options to add, modify, or delete a record.   
3. The user selects an action (add, modify, or delete) and provides the necessary details for the usage record.   
4. The system validates the input data and checks the user's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow and identifies the required approvers.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted usage record.   
8. The system logs the usage record management action in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and possibly stakeholders.   
10. The system confirms the completion of the usage record management action.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the user does not have permission to manage usage records, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the usage record change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and email notification is requested, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage PermissionRecord   
Use Case ID: UC-22   
Actors: Administrator, Authentication System, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve permission record data.   
3. The Authentication System is operational to validate user credentials and manage permissions.   
4. The Approval Workflow is configured and active if changes to permission records require approval.   
5. The Email System is functional to send notifications if required.   
6. At least one permission record must exist in the system, or the Administrator is ready to create a new one.   
  
Postconditions:   
1. The permission record is added, modified, or deleted in the Database.   
2. The change to the permission record is logged in the Audit Trail.   
3. The Approval Workflow is completed if initiated.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the permission record management action.   
  
Main Flow:   
1. The Administrator accesses the "Manage PermissionRecord" feature.   
2. The system displays a list of existing permission records and provides options to add, modify, or delete records.   
3. The Administrator selects an action (add, modify, or delete) and provides the necessary details for the permission record.   
4. The system validates the input data and checks the Administrator's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow and identifies the required approvers.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted permission record.   
8. The system logs the permission record management action in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and possibly stakeholders.   
10. The system confirms the completion of the permission record management action.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have permission to manage permission records, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the permission record change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and email notification is requested, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage AuthenticationRecord   
Use Case ID: UC-23   
Actors: Administrator, Authentication System, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve authentication record data.   
3. The Authentication System is operational to validate user credentials and manage authentication records.   
4. The Approval Workflow is configured and active if changes to authentication records require approval.   
5. The Email System is functional to send notifications if required.   
6. At least one authentication record must exist in the system, or the Administrator is ready to create a new one.   
  
Postconditions:   
1. The authentication record is added, modified, or deleted in the Database.   
2. The change to the authentication record is logged in the Audit Trail.   
3. The Approval Workflow is completed if initiated.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the authentication record management action.   
  
Main Flow:   
1. The Administrator accesses the "Manage AuthenticationRecord" feature.   
2. The system displays a list of existing authentication records and provides options to add, modify, or delete a record.   
3. The Administrator selects an action (add, modify, or delete) and provides the necessary details for the authentication record.   
4. The system validates the input data and checks the Administrator's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow and identifies the required approvers.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted authentication record.   
8. The system logs the authentication record management action in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and possibly stakeholders.   
10. The system confirms the completion of the authentication record management action.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have permission to manage authentication records, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the authentication record change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and email notification is requested, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage EmailNotification   
Use Case ID: UC-24   
Actors: Administrator, Email System, Database, Audit Trail   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve email notification configurations and settings.   
3. The Email System is operational and properly configured.   
4. The Audit Trail is available to record activities related to managing email notifications.   
5. The system supports configuration of notification recipients, templates, and trigger conditions.   
6. At least one email notification configuration exists in the system, or the Administrator is ready to create a new one.   
  
Postconditions:   
1. The email notification configuration is added, modified, or deleted in the Database.   
2. The change to the email notification is logged in the Audit Trail.   
3. The Email System is updated to reflect the new notification settings.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the email notification management action.   
  
Main Flow:   
1. The Administrator accesses the "Manage EmailNotification" feature.   
2. The system displays a list of existing email notification configurations and provides options to add, modify, or delete a configuration.   
3. The Administrator selects an action (add, modify, or delete) and provides the necessary details (e.g., event triggers, recipients, templates).   
4. The system validates the input data and checks the Administrator's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow and identifies the required approvers.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted email notification configuration.   
8. The system synchronizes the Email System with the updated notification settings.   
9. The system logs the email notification management action in the Audit Trail.   
10. The system sends a confirmation email to the Administrator and possibly stakeholders.   
11. The system confirms the completion of the email notification management action.   
12. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have permission to manage email notifications, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the email notification change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and synchronization is attempted, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.  
  
Use Case Name: Manage DataImportExportRecord   
Use Case ID: UC-25   
Actors: Administrator, Database, Audit Trail, Approval Workflow, Email System   
  
Preconditions:   
1. The Administrator is authenticated and logged into the system.   
2. The system has access to the Database to store and retrieve data import/export records.   
3. The Audit Trail is enabled to log activities related to data import/export.   
4. The Approval Workflow is configured and active if managing data import/export records requires approval.   
5. The Email System is operational to send notifications if required.   
6. At least one data import/export record must exist in the system, or the Administrator is ready to create a new one.   
7. The system supports import and export functionalities for asset-related data.   
  
Postconditions:   
1. The data import/export record is added, modified, or deleted in the Database.   
2. The change to the data import/export record is logged in the Audit Trail.   
3. The Approval Workflow is completed if initiated.   
4. A confirmation email is sent to the Administrator and possibly stakeholders via the Email System.   
5. The system confirms the successful completion of the data import/export record management action.   
  
Main Flow:   
1. The Administrator accesses the "Manage DataImportExportRecord" feature.   
2. The system displays a list of existing data import/export records and provides options to add, modify, or delete records.   
3. The Administrator selects an action (add, modify, or delete) and provides the necessary details for the data import/export record (e.g., file name, date, user, operation type, status).   
4. The system validates the input data and checks the Administrator's authority to perform the selected action.   
5. If the action requires approval, the system initiates the Approval Workflow and identifies the required approvers.   
6. The Approval Workflow is completed by authorized users.   
7. The system updates the Database with the new, modified, or deleted data import/export record.   
8. The system logs the data import/export record management action in the Audit Trail.   
9. The system sends a confirmation email to the Administrator and possibly stakeholders.   
10. The system confirms the completion of the data import/export record management action.   
11. The use case is completed.   
  
Alternative Flow:   
1. If the Administrator does not have permission to manage data import/export records, the system denies the request and logs the attempt in the Audit Trail.   
2. If the input data is invalid or incomplete, the system displays an error message and aborts the action.   
3. If the Approval Workflow is not completed within a specified timeframe, the system sends a reminder email to the approvers.   
4. If the Approval Workflow is rejected, the system cancels the data import/export record change and logs the rejection in the Audit Trail.   
5. If the Database is unavailable, the system displays an error message and aborts the management process.   
6. If the Email System is not operational and email notification is requested, the system logs an error and notifies the Administrator.   
7. If the Audit Trail fails to record the event, the system logs an error and notifies the Administrator.