项目文档

# Functional Requirement

2. Functional Requirements  
2.1 Asset Registration  
Input: Asset details (name, type, serial number, location, status).  
Output: Confirmation of successful registration and unique asset ID.  
Description: Users can register new assets into the system by entering required fields. Only authorized users may perform this action.  
2.2 Asset Modification  
Input: Updated asset information (e.g., location, status, owner).  
Output: Confirmation of updated asset record.  
Description: Authorized users can modify asset details based on predefined workflows and permissions.  
2.3 Asset Disposal  
Input: Disposal request including reason and method.  
Output: Disposal confirmation and audit log entry.  
Description: Assets can be marked as disposed of after approval through a defined workflow process.  
2.4 User Permissions and Roles  
Input: User role assignments (admin, manager, user, approver).  
Output: Permission configuration applied to user account.  
Description: The system assigns roles to users, each with specific permissions for asset-related actions.  
2.5 Approval Workflow  
Input: Request for asset action (e.g., modification, disposal).  
Output: Approval or rejection status and audit trail.  
Description: A configurable workflow engine routes requests to appropriate approvers based on role and asset type.  
2.6 Reporting and Analytics  
Input: Report criteria (date range, asset type, user).  
Output: Generated report in PDF/Excel format.  
Description: Users can generate reports on asset usage, status, ownership, and audit history.  
2.7 Data Import and Export  
Input: CSV/Excel file containing asset records.  
Output: Imported data or exported file.  
Description: The system supports bulk import of assets from external files and export of asset data for archival or reporting purposes.  
2.8 Email Integration  
Input: Event triggering notification (approval request, asset update).  
Output: Email notification sent to relevant parties.  
Description: Automated email alerts are sent when key events occur, such as pending approvals or asset changes.  
2.9 Authentication and Authorization  
Input: User credentials (username/password).  
Output: Access granted/denied based on authentication result.  
Description: The system uses a secure authentication mechanism (e.g., OAuth2, LDAP) and enforces role-based access controls.  
2.10 Audit Trail  
Input: System event (login, asset change, approval).  
Output: Log entry stored in database.  
Description: All significant system actions are logged for audit and compliance purposes.

# External Description

External Interfaces  
Interface Type Description  
Database Relational database (e.g., PostgreSQL, MySQL) for storing asset data, user roles, logs, and reports.  
Email Server SMTP server integration for sending notifications and alerts.  
Authentication Service Integration with LDAP or OAuth2 provider for user authentication.  
File Storage Local or cloud storage for imported/exported files and report outputs.