项目文档

# Functional Requirement

## 3.2 Functional Requirement List  
  
| Requirement ID | Priority | Statement | Rationale | Source | Acceptance Criteria |  
|----------------|----------|-----------|-----------|--------|---------------------|  
| \*\*ASSET-DASHBOARD-001\*\* | Must Have | The system shall provide a single, real-time dashboard consolidating all asset data (financial and physical/mobile) into one interface to eliminate the need for cross-referencing multiple systems. | Eliminate data silos and provide a unified view for operational efficiency. | FR-1 | A user can view financial and physical/mobile asset data in one screen. |  
| \*\*ASSET-SYNC-002\*\* | Must Have | The system shall automate data synchronization for asset purchases, maintenance, and user access to reduce manual effort and inconsistencies. | Ensure data accuracy and reduce administrative overhead. | FR-2 | All data changes are synchronized across integrated systems within 5 minutes. |  
| \*\*ASSET-REPORT-003\*\* | Should Have | The system shall provide a digital form for staff to report asset issues, including support for text descriptions and photo uploads. | Enable staff to report issues efficiently with visual evidence. | FR-3 | Staff can submit an issue with a photo and description via the mobile app or web. |  
| \*\*ASSET-ASSIGN-004\*\* | Must Have | The system shall automatically assign maintenance requests to appropriate personnel based on asset type and location. | Improve response time and ensure correct personnel are notified. | FR-4 | Maintenance request is assigned to the correct technician within 1 minute of submission. |  
| \*\*ASSET-APPROVAL-005\*\* | Should Have | The system shall support approval workflows, including the ability to send notifications via mobile app or email to relevant approvers. | Ensure timely approvals and reduce delays in workflows. | FR-5 | A manager receives an email and in-app notification when an approval is required. |  
| \*\*ASSET-STATUS-006\*\* | Must Have | The system shall provide real-time work order status updates and maintain a historical record of maintenance timelines. | Support visibility and accountability in maintenance processes. | FR-6 | A technician can see the current status of a work order and view its history in the system. |  
| \*\*ASSET-RBAC-007\*\* | Must Have | The system shall support role-based access control (RBAC) with predefined permission templates for different user types (e.g., staff, managers, auditors). | Enforce least-privilege access and simplify user management. | FR-7 | Predefined roles are available for staff, managers, auditors, and IT/technical staff. |  
| \*\*ASSET-ENFORCE-008\*\* | Must Have | The system shall enforce role-based permissions across all workflows and reports, ensuring that users cannot perform actions outside their designated roles. | Prevent unauthorized actions and maintain data integrity. | FR-8 | A user attempting to access a restricted feature receives an access denied message. |  
| \*\*ASSET-ACCESS-009\*\* | Should Have | The system shall allow department-level access restrictions, enabling managers and administrators to control access to specific asset groups or reports. | Support granular access control for better asset governance. | FR-9 | A manager can restrict access to a subset of assets or reports for a department. |  
| \*\*ASSET-READ-010\*\* | Must Have | The system shall provide read-only access to auditors for all asset-related data and logs to support compliance and oversight. | Ensure auditors can access data without modifying it. | FR-10 | An auditor can view asset status and logs but cannot edit or submit any form. |  
| \*\*ASSET-TRACK-011\*\* | Must Have | The system shall integrate real-time GPS and IoT data to track mobile assets (e.g., delivery vehicles). | Enable real-time visibility of mobile assets for operational control. | FR-11 | A mobile asset’s current location is displayed in the dashboard with GPS precision. |  
| \*\*ASSET-SENSOR-012\*\* | Should Have | The system shall update asset status automatically based on sensor data (e.g., tampering, door status). | Improve asset monitoring by leveraging IoT data. | FR-12 | An asset’s status changes from "active" to "tampered" when a sensor detects tampering. |  
| \*\*ASSET-REPORT-013\*\* | Should Have | The system shall allow users to generate customizable reports tailored to different stakeholder needs. | Support diverse reporting requirements and decision-making. | FR-13 | A user can select report filters (e.g., asset type, department) and export the report. |  
| \*\*ASSET-ANOMALY-014\*\* | Should Have | The system shall support automated anomaly detection in reports to highlight unusual asset behavior or performance issues. | Enhance proactive maintenance and compliance readiness. | FR-14 | A report highlights anomalies in asset usage, such as unexpected location changes. |  
| \*\*ASSET-IMPORT-015\*\* | Should Have | The system shall enable automated import and export of asset data in CSV, Excel, and JSON formats. | Support data migration and external reporting. | FR-15 | A user can import a CSV file containing new asset data and validate it in the system. |  
| \*\*ASSET-INT-016\*\* | Must Have | The system shall integrate with external tools such as Microsoft Outlook, SharePoint, SQL Server, and ERP systems. | Enable seamless workflow with existing enterprise tools. | FR-16 | A maintenance request is synchronized with an Outlook calendar event for the assigned technician. |  
| \*\*ASSET-REQ-017\*\* | Must Have | When a staff member reports an asset issue, the system shall generate a maintenance request and assign it to the appropriate personnel based on asset type and location. | Reduce response time and streamline issue resolution. | FR-17 | A maintenance request is created and assigned to a technician upon staff submission. |  
| \*\*ASSET-NOTIFY-018\*\* | Should Have | The system shall notify the manager via mobile app or email when an approval is required for a maintenance request. | Ensure timely approvals and reduce bottlenecks. | FR-18 | A manager receives a push notification and email when a request requires their approval. |  
| \*\*ASSET-UPDATE-019\*\* | Must Have | The system shall allow a technician to receive assigned work orders and update the status in real-time. | Improve maintenance workflow transparency and efficiency. | FR-19 | A technician can update a work order status from "in progress" to "completed" in real-time. |  
| \*\*ASSET-OWNERSHIP-020\*\* | Must Have | When an asset is checked out, the system shall record the user ownership and track the asset’s real-time location. | Ensure accountability and visibility during asset checkout. | FR-20 | The system records the checkout user and GPS location of the asset. |  
| \*\*ASSET-ALERT-021\*\* | Must Have | The system shall send alerts if an asset is overdue or moved outside its allowed zone. | Prevent asset misuse and ensure compliance with usage policies. | FR-21 | An alert is sent to the manager and technician when an asset is moved beyond its permitted zone. |  
| \*\*ASSET-ROLE-022\*\* | Must Have | When a new user is added, the system shall assign a predefined role and enforce the associated permissions across all system functions. | Simplify onboarding and ensure consistent access controls. | FR-22 | A new user is assigned a role with the correct permissions upon creation. |  
| \*\*ASSET-OFFLINE-023\*\* | Should Have | The system shall support mobile access and offline data entry for field users to ensure usability in scenarios without internet connectivity. | Enable field operations in low-connectivity environments. | FR-23 | A field user can submit an asset issue form offline and sync it when connectivity is restored. |

# External Description

## 5.1 Regulatory and Legal Constraints  
  
- \*\*CON-REG-001\*\*: The system shall comply with the General Data Protection Regulation (GDPR) for the handling and protection of personal data.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: The organization operates in a regulated industry and must ensure all data processing is GDPR-compliant to avoid legal penalties and reputational damage.  
 - \*\*Source\*\*: SRL-4.2-004  
 - \*\*Acceptance Criteria\*\*: GDPR compliance is verified by an external audit and confirmed by the legal department.  
  
- \*\*CON-REG-002\*\*: The system shall comply with the Service Organization Control (SOC 2) standards for data security and availability.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: SOC 2 compliance is required for the system to be considered suitable for handling sensitive data in a secure and reliable manner.  
 - \*\*Source\*\*: SRL-4.2-004  
 - \*\*Acceptance Criteria\*\*: SOC 2 Type II certification is obtained for the system.  
  
- \*\*CON-REG-003\*\*: The system shall comply with the Sarbanes-Oxley Act (SOX) for financial asset tracking and reporting.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: SOX compliance is essential to ensure the integrity and accuracy of financial data, which is a core requirement for the system.  
 - \*\*Source\*\*: SRL-4.2-004  
 - \*\*Acceptance Criteria\*\*: SOX compliance is confirmed by an independent financial audit.  
  
## 5.2 Hardware Constraints  
  
- \*\*CON-HW-001\*\*: The system shall be designed to operate in both cloud and on-premises environments.  
 - \*\*Priority\*\*: Should Have  
 - \*\*Rationale\*\*: Flexibility in deployment environments allows the system to adapt to the organization's infrastructure preferences and compliance requirements.  
 - \*\*Source\*\*: SRL-5.1-001  
 - \*\*Acceptance Criteria\*\*: Cloud and on-premises deployment options are successfully tested and documented.  
  
- \*\*CON-HW-002\*\*: The system shall support client-side access on standard desktop computers and mobile devices (iOS and Android).  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: Mobile and desktop support is critical to accommodate the needs of field users and remote staff.  
 - \*\*Source\*\*: SRL-5.1-002  
 - \*\*Acceptance Criteria\*\*: The system is successfully installed and operated on iOS and Android devices and major desktop platforms.  
  
## 5.3 Interface Constraints  
  
- \*\*CON-INT-001\*\*: The system shall integrate with Microsoft SQL Server, Oracle, and PostgreSQL databases.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: Integration with these databases is necessary to maintain data consistency and enable data synchronization with legacy systems.  
 - \*\*Source\*\*: SRL-5.3-003  
 - \*\*Acceptance Criteria\*\*: The system successfully connects and exchanges data with all three database systems.  
  
- \*\*CON-INT-002\*\*: The system shall support pre-configured integration tools to minimize custom development.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: The organization has limited IT resources for custom integration, so leveraging pre-configured tools is essential to reduce development effort and ensure timely deployment.  
 - \*\*Source\*\*: SRL-2.4-003  
 - \*\*Acceptance Criteria\*\*: Integration is achieved using pre-configured tools without requiring custom code development.  
  
- \*\*CON-INT-003\*\*: The system shall integrate with Microsoft Outlook for calendar and notification synchronization.  
 - \*\*Priority\*\*: Should Have  
 - \*\*Rationale\*\*: Outlook integration enhances user productivity by enabling calendar-based maintenance scheduling and notification management.  
 - \*\*Source\*\*: SRL-5.3-004  
 - \*\*Acceptance Criteria\*\*: Outlook integration is successfully implemented and verified in a test environment.  
  
- \*\*CON-INT-004\*\*: The system shall integrate with SharePoint for document storage and access.  
 - \*\*Priority\*\*: Should Have  
 - \*\*Rationale\*\*: SharePoint integration ensures seamless access to asset documentation and maintains data integrity across systems.  
 - \*\*Source\*\*: SRL-5.3-005  
 - \*\*Acceptance Criteria\*\*: The system successfully synchronizes and accesses documents from SharePoint.  
  
## 5.4 Design and Implementation Constraints  
  
- \*\*CON-DES-001\*\*: The system shall support single sign-on (SSO) capabilities to reduce password fatigue and improve security.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: SSO is a key requirement to streamline user authentication and reduce the risk of weak passwords or identity theft.  
 - \*\*Source\*\*: SRL-5.5-002  
 - \*\*Acceptance Criteria\*\*: SSO is implemented and verified using at least one identity provider (e.g., Azure AD).  
  
- \*\*CON-DES-002\*\*: The system shall integrate with existing identity systems such as Active Directory and LDAP.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: Integration with existing identity systems is required to ensure compatibility with the organization’s current authentication infrastructure.  
 - \*\*Source\*\*: SRL-5.5-003  
 - \*\*Acceptance Criteria\*\*: The system successfully authenticates users against Active Directory and LDAP.  
  
- \*\*CON-DES-003\*\*: The system shall support offline data entry and synchronization when connectivity is restored.  
 - \*\*Priority\*\*: Should Have  
 - \*\*Rationale\*\*: Offline functionality is essential for field users who may operate in areas with limited or no internet access.  
 - \*\*Source\*\*: SRL-5.7-002  
 - \*\*Acceptance Criteria\*\*: The system allows offline data entry and synchronizes data upon reconnection in a test environment.  
  
## 5.5 Other Constraints  
  
- \*\*CON-OTH-001\*\*: The system shall retain access logs for at least six months and allow export for audit purposes.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: Retaining and exporting logs is a compliance requirement for internal and external audits.  
 - \*\*Source\*\*: SRL-5.6-002  
 - \*\*Acceptance Criteria\*\*: Access logs are retained for six months and can be exported in CSV and PDF formats.  
  
- \*\*CON-OTH-002\*\*: The system shall support secure, real-time data transmission over HTTPS.  
 - \*\*Priority\*\*: Must Have  
 - \*\*Rationale\*\*: HTTPS is required to protect data during transmission and meet security and compliance standards.  
 - \*\*Source\*\*: SRL-5.3-001  
 - \*\*Acceptance Criteria\*\*: All data transmission is encrypted using HTTPS, verified through network traffic analysis.