# Functional Requirement

### 1.1 Asset Registration Function

\*\*Function Number: FR-01\*\*

\*\*Description\*\*: After system authentication, users can fill in basic asset information and upload supporting documents. The system automatically generates a unique asset identification code and triggers the approval process.

\*\*Input\*\*: Basic asset information (name, category, specifications, purchase date, etc.), supporting documents (contract/invoice scans), user authentication information.

\*\*Output\*\*: Unique asset identification code, asset information record, approval task pushed to the approval queue, registration success prompt.

### 1.2 Asset Transfer Function

\*\*Function Number: FR-02\*\*

\*\*Description\*\*: After two - factor authentication, users can initiate asset transfer requests and select the receiving department. The system generates a transfer record and triggers a multi - level approval process.

\*\*Input\*\*: List of transferable assets, receiving department information, reason for transfer, expected handover date, transfer voucher (transfer order scan).

\*\*Output\*\*: Asset status updated to "in transfer," cross - department transfer record generated, multi - level approval process initiated, in - app notification to approvers.

### 1.3 Asset Return Function

\*\*Function Number: FR-03\*\*

\*\*Description\*\*: After biometric authentication, users can submit asset return requests and upload photos of the current asset status. The system generates a return record and triggers the acceptance process.

\*\*Input\*\*: List of assets currently held by the user, return type, usage explanation, current asset status photos, return date.

\*\*Output\*\*: Asset status updated to "awaiting acceptance," physical acceptance task work order generated, user - asset binding removed, maintenance process triggered.

### 1.4 Asset Information Modification Function

\*\*Function Number: FR-04\*\*

\*\*Description\*\*: After dynamic token authentication, users can modify asset information. The system generates version comparisons and triggers corresponding approval processes based on the sensitivity of the changes.

\*\*Input\*\*: Asset information change fields (name, category, specifications, net value, depreciation method, custodian, storage location), change explanation, user authentication information.

\*\*Output\*\*: Updated asset information version, modification audit record, data synchronized with related systems, modification confirmation notification.

### 1.5 Asset Information Management Function

\*\*Function Number: FR-05\*\*

\*\*Description\*\*: After digital certificate authentication, users can view the full - life - cycle view of assets, adjust information display dimensions, and configure automatic alert rules.

\*\*Input\*\*: Asset information management operation type (basic information maintenance, status change tracking, relationship configuration, historical record tracing), asset tree navigation selection, user authentication information.

\*\*Output\*\*: Updated asset information, asset health assessment report, multi - dimensional information dashboard update, audit system operation trajectory push.

### 1.6 Asset Data Import Function

\*\*Function Number: FR-06\*\*

\*\*Description\*\*: After two - factor authentication, users can upload standard template files. The system parses and validates the data and performs batch import operations.

\*\*Input\*\*: Standard template file (Excel/CSV format), conflict resolution strategy, null value handling method, user authentication information.

\*\*Output\*\*: Persistent storage of asset data, data validation report, data import index update, data quality analysis report.

### 1.7 Asset Data Export Function

\*\*Function Number: FR-07\*\*

\*\*Description\*\*: After digital signature authentication, users can configure export parameters and export data. The system generates encrypted files and embeds watermark information.

\*\*Input\*\*: Data export parameters (scope, fields, format), file protection measures (password, watermark, automatic destruction time), user authentication information.

\*\*Output\*\*: Encrypted data file, operation audit record, data export behavior analysis report, data watermark identifier update.

### 1.8 Asset Deletion Function

\*\*Function Number: FR-08\*\*

\*\*Description\*\*: After three - factor authentication, users can delete assets that meet the deletion criteria. The system performs secure erasure and generates irreversible deletion logs.

\*\*Input\*\*: List of assets to be deleted, deletion type (logical deletion/physical destruction), reason for deletion, destruction voucher, user authentication information.

\*\*Output\*\*: Asset status updated to "marked for deletion," deletion operation log, cross - system data archiving process triggered, permanent deletion operation executed.

### 1.9 User Addition Function

\*\*Function Number: FR-09\*\*

\*\*Description\*\*: After multi - factor authentication, administrators can add new user information, configure permissions, and trigger the approval process.

\*\*Input\*\*: Basic user information (name, employee number, department), permission configuration (preset role template or custom permissions), asset binding information, user authentication information.

\*\*Output\*\*: User account creation, permission configuration, permission approval process triggered, user activation notification.

### 1.10 User Information Editing Function

\*\*Function Number: FR-10\*\*

\*\*Description\*\*: After two - factor authentication, users can edit basic information. The system triggers the approval process based on the changes and updates related system data.

\*\*Input\*\*: Basic user information (name, contact information, department), security information (password, security questions), permission information (functional permissions, data permissions), user authentication information.

\*\*Output\*\*: User information change trajectory, permission change approval process triggered, related system data synchronization, modification confirmation notification.

### 1.11 User Information Management Function

\*\*Function Number: FR-11\*\*

\*\*Description\*\*: After dynamic password authentication, administrators can view, modify, freeze, or delete user information. The system synchronizes and updates permissions and identity data.

\*\*Input\*\*: User information management operation type (query, modify, freeze, delete), permission adjustment parameters, user authentication information.

\*\*Output\*\*: Updated user information, permission impact analysis report, identity data synchronization, audit system evidence - keeping.

### 1.12 User Deletion Function

\*\*Function Number: FR-12\*\*

\*\*Description\*\*: After four - factor authentication, administrators can delete users that meet the deletion criteria. The system performs secure erasure and generates irreversible deletion logs.

\*\*Input\*\*: List of users to be deleted, deletion mode (immediate deletion/timed destruction), deletion basis, user authentication information.

\*\*Output\*\*: User status updated to "marked for deletion," deletion operation audit chain, identity information archiving process triggered, physical destruction operation executed.

### 1.13 Administrator Addition Function

\*\*Function Number: FR-13\*\*

\*\*Description\*\*: After five - factor authentication, system administrators can add new administrator accounts and configure permissions. The system performs secure initialization and generates the approval process.

\*\*Input\*\*: Basic administrator information (ID, name, department), permission scope, authentication method, administrator authentication information.

\*\*Output\*\*: Administrator account creation, permission configuration, secure initialization, approval process triggered.

### 1.14 Administrator Information Editing Function

\*\*Function Number: FR-14\*\*

\*\*Description\*\*: After quantum encryption authentication, system administrators can edit administrator account information. The system performs permission conflict detection and generates the approval process.

\*\*Input\*\*: Administrator information modification content (digital certificate, permission topology, biometrics), approver configuration, administrator authentication information.

\*\*Output\*\*: Updated administrator information, permission topology adjustment, approval process triggered, audit system evidence - keeping.

### 1.15 Administrator Information Management Function

\*\*Function Number: FR-15\*\*

\*\*Description\*\*: After five - factor authentication, system administrators can manage the lifecycle of administrator accounts. The system performs data integrity verification and synchronizes permission data.

\*\*Input\*\*: Administrator information management operation type (correction, archiving, cleanup, verification), management parameters, administrator authentication information.

\*\*Output\*\*: Updated administrator status, blockchain evidence - keeping, cross - system permission synchronization, management impact analysis report.

### 1.16 Administrator Deletion Function

\*\*Function Number: FR-16\*\*

\*\*Description\*\*: After six - factor authentication, system administrators can delete administrator accounts and clear all permission traces. The system performs data annihilation and generates irreversible deletion logs.

\*\*Input\*\*: List of administrators to be deleted, deletion type (logical marking/physical destruction/quantum annihilation), reason for deletion, administrator authentication information.

\*\*Output\*\*: Administrator status updated to "quantum erasure," deletion operation log, permission topology reconstruction, business system update.

### 1.17 Permission Allocation Function

\*\*Function Number: FR-17\*\*

\*\*Description\*\*: After three - factor authentication, administrators can allocate permissions to users. The system performs conflict detection and generates the approval process.

\*\*Input\*\*: Target user information, permission configuration (template inheritance or custom), approver configuration, administrator authentication information.

\*\*Output\*\*: Updated user permissions, permission change blockchain evidence - keeping, cross - system permission synchronization, permission activation notification.

### 1.18 Permission Management Function

\*\*Function Number: FR-18\*\*

\*\*Description\*\*: After four - factor authentication, administrators can manage the permission architecture. The system performs permission conflict detection and generates the approval process.

\*\*Input\*\*: Permission management operation type (addition, adjustment, cleanup, restoration), permission configuration parameters, administrator authentication information.

\*\*Output\*\*: Updated permission architecture, permission impact analysis report, cross - system data synchronization, dual - person review audit log.

### 1.19 Approval Process Handling Function

\*\*Function Number: FR-19\*\*

\*\*Description\*\*: After users or administrators submit approval requests, the system automatically matches approval rules, executes the multi - level approval process, and updates the approval status.

\*\*Input\*\*: Approval request information, approval type, approver configuration, approver authentication information.

\*\*Output\*\*: Updated approval status, approval operation log, business object status update, approval result notification.

### 1.20 Approval Record Query Function

\*\*Function Number: FR-20\*\*

\*\*Description\*\*: After two - factor authentication, users can configure multi - dimensional query conditions. The system returns approval records and performs access control.

\*\*Input\*\*: Query conditions (approval type, time range, approval number, approval status), user authentication information.

\*\*Output\*\*: Returned approval records, query trajectory log, visual analysis results, abnormal query behavior analysis.

### 1.21 Approval Record Management Function

\*\*Function Number: FR-21\*\*

\*\*Description\*\*: After three - factor authentication, administrators can perform archiving, desensitization, and cleanup operations on approval records and generate management logs.

\*\*Input\*\*: Approval record management operation type (archiving, desensitization, cleanup, verification), management parameters, administrator authentication information.

\*\*Output\*\*: Updated approval record status, blockchain evidence - keeping, data synchronization, management impact analysis report.

### 1.22 Asset Transfer Record Viewing Function

\*\*Function Number: FR-22\*\*

\*\*Description\*\*: After two - factor authentication, users can view asset transfer records. The system provides multi - dimensional queries and visual displays.

\*\*Input\*\*: Query conditions (time range, asset code, department, status), user authentication information.

\*\*Output\*\*: Returned asset transfer records, visual charts, audit logs, abnormal query behavior analysis.

### 1.23 Asset Return Record Viewing Function

\*\*Function Number: FR-23\*\*

\*\*Description\*\*: After two - factor dynamic authentication, users can view asset return records. The system provides multi - dimensional queries and visual displays.

\*\*Input\*\*: Query conditions (time range, asset serial number, return type, acceptance result), user authentication information.

\*\*Output\*\*: Returned asset return records, visual charts, audit logs, abnormal access pattern analysis.

### 1.24 Asset Transfer Record Management Function

\*\*Function Number: FR-24\*\*

\*\*Description\*\*: After three - factor authentication, administrators can correct, archive, and clean up asset transfer records. The system performs approval and generates management logs.

\*\*Input\*\*: Management operation type (correction, archiving, cleanup, verification), management parameters, administrator authentication information.

\*\*Output\*\*: Updated asset transfer records, approval process triggered, data synchronization, management impact analysis report.

### 1.25 Asset Return Record Management Function

\*\*Function Number: FR-25\*\*

\*\*Description\*\*: After four - factor authentication, administrators can correct, archive, and erase asset return records. The system performs integrity verification and generates management logs.

\*\*Input\*\*: Management operation type (correction, archiving, erasure, verification), management parameters, administrator authentication information.

\*\*Output\*\*: Updated asset return records, blockchain evidence - keeping, cross - system data synchronization, management impact analysis heatmap.