# Functional Requirement

## 1.1 Email Sending Function

Function ID: FR-01

Description: Authenticated users can compose and send emails via the system, supporting rich-text editing, attachment addition, scheduled sending, and read-receipt settings.

Input: Recipient address, email subject, body content, attachment list, send time, read-receipt option.

Output: Sent email record, outbox status update, operation log entry.

## 1.2 Email Receiving Function

Function ID: FR-02

Description: The system must monitor the mail server in real time or poll periodically to receive new emails, performing spam filtering, sender verification, email classification, and triggering notifications.

Input: Mail server status, new email data, anti-spam policy parameters, user notification preferences.

Output: Inbox email records, spam email records, unread count update, user notifications.

## 1.3 Email Management Function

Function ID: FR-03

Description: Users can mark, archive, move, or delete emails; the system must synchronize email status and storage location updates.

Input: Target email list, action type (mark/archive/move/delete, etc.), target folder/archive policy.

Output: Email status update, folder structure change, storage space status refresh, operation log entry.

## 1.4 Email Search Function

Function ID: FR-04

Description: Users can search emails using keywords, time ranges, sender/recipient, etc.; the system must return a list of matching emails.

Input: Search keywords, filter criteria (time, sender, recipient, email status, etc.), search scope (inbox, sent, etc.).

Output: Matching email list, search result ranking, highlighted matches, search statistics.

## 1.5 Email Folder Management Function

Function ID: FR-05

Description: Users can create, rename, and delete email folders, set folder attributes, and configure auto-archiving policies.

Input: Parent folder, folder name, folder attributes (color label, access permissions), auto-archiving rules.

Output: Folder tree update, folder attribute configuration, email index path mapping, operation log entry.

## 1.6 Contact Management Function

Function ID: FR-06

Description: Users can create, edit, and delete contacts, and link them to distribution groups; the system must provide intelligent deduplication and offline saving.

Input: Contact info (name, email, phone, etc.), associated distribution group, action type (create/edit/delete).

Output: Contact list update, distribution group membership change, operation log entry, data integrity check.

## 1.7 Distribution Group Management Function

Function ID: FR-07

Description: Users can create and manage distribution groups, set members, visibility, email approval rules, and recipient limits.

Input: Group name, member list, visibility scope, approval rules, sending limit.

Output: Distribution group list update, membership change, group email rules sync, operation log entry.

## 1.8 Calendar Creation Function

Function ID: FR-08

Description: Authenticated users can create personal or shared calendars and configure default view, auto-reminders, and sync devices.

Input: Calendar name, color label, sharing scope, default view, timezone setting.

Output: New calendar record, calendar index update, auto-reminder rule sync, operation log entry.

## 1.9 Calendar Event Management Function

Function ID: FR-09

Description: Users can add, modify, or delete events in the calendar and set event reminders and recurrence rules.

Input: Event title, time range, location, attendees, reminder method, recurrence rule.

Output: Calendar event record update, reminder task sync, attendee status sync, operation log entry.

## 1.10 Reminder Task Management Function

Function ID: FR-10

Description: Users can create, edit, or delete reminder tasks and associate them with emails, calendar events, etc., supporting multiple reminder methods (email, pop-up, SMS).

Input: Reminder description, trigger time, linked content (email/event), reminder method, recurrence rule.

Output: Reminder task record update, reminder queue sync, notification channel config, operation log entry.

## 1.11 User Login Function

Function ID: FR-11

Description: Users log in with username and password, supporting multi-factor authentication (dynamic code, biometrics) and third-party authentication.

Input: Username, password, verification code, device info, auth method selection.

Output: Access token, user preference loading, login status record, security log update.

## 1.12 User Logout Function

Function ID: FR-12

Description: Users can securely log out; the system must terminate the session, release resources, and handle unsaved data.

Input: Logout request, unsaved data status, device info.

Output: Session termination, sensitive data clearance, residual data handling, login status reset.

## 1.13 User Account Management Function

Function ID: FR-13

Description: Admins can create, delete, and modify user accounts and adjust user permissions, storage quotas, and password policies.

Input: User info (name, email, department), account status (enabled/disabled), permission group, storage quota, password policy.

Output: User list update, permission sync, storage quota adjustment, operation log entry.

## 1.14 Archive Management Function

Function ID: FR-14

Description: Users can archive emails to designated directories; the system must execute archiving, retention, and cleanup per policy and log archiving actions.

Input: Email list to archive, target archive directory, retention policy, conflict handling option.

Output: Archive directory update, email status change, archiving metadata record, operation log update.

## 1.15 Archive Policy Management Function

Function ID: FR-15

Description: Admins can create, modify, and delete archive policies, define rules, retention periods, and storage tiers, ensuring policy compliance.

Input: Policy name, archive rules, retention period, storage tier, effective time.

Output: Archive policy record update, policy impact analysis report, storage space estimate, operation log entry.

## 1.16 Data Backup Function

Function ID: FR-16

Description: The system must back up emails, calendars, contacts, etc., per backup policy and generate backup logs.

Input: Backup policy, data scope, encryption settings, storage location.

Output: Backup copy, backup log, storage space status update, integrity check report.

## 1.17 Data Recovery Function

Function ID: FR-17

Description: Users or admins can recover data from backup copies, supporting recovery by time point, data type, and storage location.

Input: Recovery policy, target recovery point (time/backup ID), recovery scope, conflict handling option.

Output: Recovered data status, storage space update, recovery log entry, integrity check result.

## 1.18 Backup Log Management Function

Function ID: FR-18

Description: Admins can view, analyze, and export backup logs to ensure backup traceability.

Input: Log filter criteria (time, type, backup policy), export format, storage location.

Output: Backup log list, visualization report, export file, audit log update.

## 1.19 Recovery Log Management Function

Function ID: FR-19

Description: Admins can view, analyze, and export recovery logs to ensure recoverability and auditability.

Input: Log filter criteria (recovery type, time, operator), export format, storage location.

Output: Recovery log list, recovery performance report, export file, audit log update.

## 1.20 Data Integrity Check Function

Function ID: FR-20

Description: The system must perform integrity checks on emails, calendar events, contacts, backup copies, etc., to ensure data consistency.

Input: Data scope, check algorithm (SHA-256/SHA-3), check frequency, storage location.

Output: Integrity check result, discrepancy record, data repair suggestion, operation log update.

## 1.21 Operation Log Recording Function

Function ID: FR-21

Description: The system must log all user and admin operations, including email sending, archiving, recovery, etc., ensuring traceability.

Input: Operation type, operation object, timestamp, operator identity, original data state.

Output: Operation log entry, log index update, audit report generation, privilege violation record.

## 1.22 Storage Quota Management Function

Function ID: FR-22

Description: The system must manage user mailbox and storage quotas, provide real-time usage statistics, and smart cleanup suggestions.

Input: User quota settings, storage usage, cleanup policy.

Output: Quota usage status, cleanup suggestions, quota adjustment record, storage health report.

## 1.23 Data Classification & Tagging Function

Function ID: FR-23

Description: Users can assign classification tags to emails, contacts, calendar events, etc.; the system must support tag search and management.

Input: Tag name, associated data (email/contact/event), tag classification rules.

Output: Tag list update, data index optimization, tag management interface refresh, operation log entry.

## 1.24 Notification & Reminder Service Function

Function ID: FR-24

Description: The system must trigger reminder notifications via email, pop-up, SMS, etc., based on user-defined reminder tasks.

Input: Reminder task list, trigger time, notification method, user preference settings.

Output: Notification send status, reminder task execution record, user feedback log, operation log entry.

## 1.25 Security Audit & Compliance Function

Function ID: FR-25

Description: The system must log all sensitive operations, including privilege abuse, data deletion, backup and recovery, and ensure regulatory compliance.

Input: Sensitive operation type, data scope, operation time, operator identity.

Output: Security audit report, compliance verification result, privilege-abuse record, regulatory clause reference.

## 1.26 System Maintenance & Health Check Function

Function ID: FR-26

Description: Admins can perform system maintenance, including service restart, health checks, storage cleanup, and log archiving.

Input: Maintenance action type (restart/health check/cleanup/archive), impact scope, execution time.

Output: System status report, maintenance operation log, storage health status, service availability verification.

## 1.27 System Monitoring & Alert Function

Function ID: FR-27

Description: The system must monitor real-time status of email, calendar, contact, and backup modules, and trigger alerts on anomalies.

Input: Monitoring metrics (storage usage, service response time, error rate), alert thresholds, notification method.

Output: System health dashboard, alert notification, anomaly event record, maintenance suggestion.

## 1.28 Data Encryption & Decryption Function

Function ID: FR-28

Description: The system must encrypt sensitive data (email body, attachments, backup files) and support decryption requests by users or admins.

Input: Encryption algorithm (AES-256), key version, data scope to encrypt, decryption request.

Output: Encrypted data storage, decrypted data access, encryption policy record, key usage log.

## 1.29 Data Versioning Function

Function ID: FR-29

Description: The system must provide versioning for emails, calendars, distribution groups, backups, etc., supporting historical version viewing and rollback.

Input: Data object (email/calendar/group), version selection, rollback option.

Output: Version history record, data rollback status, version snapshot, operation log entry.

## 1.30 Bulk Distribution Group Management Function

Function ID: FR-30

Description: Admins can bulk import/export distribution group data with conflict detection and data-cleanup mechanisms.

Input: Distribution group file (CSV/Excel), action type (import/export), field mapping, processing policy.

Output: Distribution group list update, error report, storage space status, operation log entry.

## 1.31 Email Attachment Management Function

Function ID: FR-31

Description: Users can add, delete, and preview email attachments; the system must validate file size and format and support encrypted attachment access.

Input: Attachment file, file format, file size, attachment access request (decrypt).

Output: Attachment list update, attachment status (available/unavailable), encrypted-access approval record, operation log entry.

## 1.32 Timezone & Time Sync Function

Function ID: FR-32

Description: The system must adjust and sync time displays for emails, calendar events, and reminders based on user timezone settings.

Input: User timezone setting, calendar time range, reminder task time, timeline navigation request.

Output: Time display adjustment, time-sync record, cross-timezone event handling, timezone conversion report.

## 1.33 Data Export Function

Function ID: FR-33

Description: Users or admins can export emails, contacts, distribution groups, calendar events, etc., in various formats with encryption options.

Input: Export scope (email/contact/calendar), export format (CSV/Excel/vCard), encryption settings, field selection.

Output: Export file, export operation log, integrity check report, storage space update.

## 1.34 Data Recovery Log Function

Function ID: FR-34

Description: The system must log all recovery operations in detail, ensure logs are tamper-proof, and support audit trails.

Input: Recovery operation details, recovery timestamp, data scope, operator identity.

Output: Recovery log entry, recovery status update, audit report, integrity check.

## 1.35 User Permission Management Function

Function ID: FR-35

Description: The system must manage user permissions to ensure users can only access data and functions within their scope.

Input: User role, functional permissions, data-access permissions, permission-change request.

Output: Permission config update, permission-conflict record, permission log, privilege-abuse audit record.

## 1.36 Email Classification & Filtering Function

Function ID: FR-36

Description: The system must support email classification (spam/important/starred) and filtering (by sender, keyword, time) to help users quickly locate emails.

Input: Filter criteria (keyword, sender, time), classification tags, email list filter request.

Output: Classified email list, filter result, classification rule record, operation log update.

## 1.37 Auto Data Cleanup Function

Function ID: FR-37

Description: The system must automatically clean expired or invalid data per archive and backup policies to ensure efficient storage usage.

Input: Cleanup policy, data scope (email/calendar/archive), cleanup frequency, retention rules.

Output: Cleanup task execution record, storage space update, data status change, operation log entry.

## 1.38 Login Security Detection Function

Function ID: FR-38

Description: The system must detect anomalies such as device fingerprint and geolocation on user login, triggering secondary verification to secure the account.

Input: Login device info, IP address, geolocation, login history.

Output: Login security assessment, secondary-verification trigger, device-fingerprint record, login status update.

## 1.39 Backup & Recovery Consistency Check Function

Function ID: FR-39

Description: The system must verify consistency between backup and recovery data to ensure data integrity.

Input: Backup ID, recovery ID, check algorithm (SHA-256), check scope.

Output: Consistency check report, discrepancy record, data-repair suggestion, operation log update.

## 1.40 System Exception Handling Function

Function ID: FR-40

Description: The system must handle operation exceptions (insufficient privilege, storage failure, network interruption) to ensure rollback and data consistency.

Input: Exception event type, affected data, recovery policy, operator identity.

Output: Exception handling record, operation rollback status, system-recovery report, security audit log.