# Functional Requirement

2. Email Communication Function

2.1 Email Sending Function

Function ID: FR-01

Description: Users can create and send emails within the system. The system must validate the recipient's address, attachment size, and sender's identity, and deliver the email to the server via the SMTP protocol.

Input: Recipient's email address, email subject, body content, attachments (optional).

Output: Update the sending record in the outbox, update the email flow log, trigger the archiving policy categorization, update the backup log.

2.2 Email Receiving Function

Function ID: FR-02

Description: The system must periodically poll the email server to receive new emails, perform anti-spam filtering, email categorization, and virus detection, and update the inbox and email flow log.

Input: Email server polling request, email data packet, SPF/DKIM validation results.

Output: Store new emails in the inbox, trigger the archiving policy categorization, generate unread email notifications, update the email flow log.

2.3 Email Search Function

Function ID: FR-03

Description: Users can construct multi-condition searches, including keywords, time ranges, sender/recipient filtering, and attachment type filtering, and obtain a set of matching email results.

Input: Search criteria (keywords, time range, sender/recipient, attachment type).

Output: Matching email list, search result cache, generate search behavior analysis report.

3. Folder Management Function

3.1 Create Folder Function

Function ID: FR-04

Description: Users can create new folders and configure permissions, shared account binding, and archiving policy association.

Input: Folder name, parent folder, permission configuration, shared account binding, archiving policy binding.

Output: Write folder metadata to the database, update the tree navigation, synchronize to the backup mirror, trigger the archiving policy evaluation.

3.2 Rename Folder Function

Function ID: FR-05

Description: Users can rename existing folders and synchronize the update of all related paths and indexes.

Input: Folder ID, new folder name, permission verification result.

Output: Updated folder metadata, refresh the folder tree structure, synchronize to mobile devices, update the archiving policy binding status.

3.3 Delete Folder Function

Function ID: FR-06

Description: Users can delete folders and, based on the selected method, permanently delete the data or move it to the recycle bin. The system must update the storage quota and access control list.

Input: Folder ID, deletion method (permanent/move to recycle bin), permission verification result.

Output: Update folder status, release storage space, synchronize to the backup mirror, update the archiving policy binding.

4. Contact Management Function

4.1 Create Contact Function

Function ID: FR-07

Description: Users can create new contacts and configure basic information, such as name, email, phone number, and the associated contact group.

Input: Contact basic information (name, email, phone number), contact group association, shared account permissions.

Output: Write contact data to the database, update the contact group member directory, trigger the archiving policy synchronization, generate audit logs.

4.2 Edit Contact Information Function

Function ID: FR-08

Description: Users can modify contact information, including email, phone number, and associated permissions, and synchronize the updates to the contact group and email client.

Input: Contact ID, modified field values, permission verification result.

Output: Updated contact information, update the contact group member directory, refresh the email auto-complete cache, generate a modification difference report.

4.3 Delete Contact Function

Function ID: FR-09

Description: Users can delete contact information and disassociate it from contact groups, tasks, and shared accounts.

Input: Contact ID, deletion method (permanent/recycle bin), permission verification result.

Output: Update contact status, update the contact group member directory, clear the email auto-complete cache, terminate associated reminder tasks.

5. Contact Group Management Function

5.1 Create Contact Group Function

Function ID: FR-10

Description: Administrators can create contact groups, supporting static groups (manually maintained) and dynamic groups (rule-based).

Input: Contact group name, type (static/dynamic), member selection method, archiving policy binding, shared permission configuration.

Output: Write contact group information to the database, update the contact group structure tree, trigger the email client auto-complete cache refresh.

5.2 Manage Contact Group Members Function

Function ID: FR-11

Description: Contact group managers can add or remove members and adjust the filtering rules for dynamic groups.

Input: Contact group ID, member change operation (add/remove), dynamic group filtering rule modification.

Output: Update the contact group member list, update the archiving policy, refresh the email auto-complete cache, generate a member change log.

5.3 Export Contact Group Members Function

Function ID: FR-12

Description: Users can export contact group members in a specified format, such as CSV, vCard, etc., and support encrypted export.

Input: Contact group ID, export format selection, encryption configuration (optional).

Output: Generate and provide the export file for download, update the export operation log, synchronize to the server archive.

6. Task Management Function

6.1 Create Task Function

Function ID: FR-13

Description: Users can create new tasks and set the task title, priority, due date, reminder rules, and collaboration attributes.

Input: Task title, priority, due date, task description, reminder rules, participant configuration.

Output: Write task information to the database, create reminder timeline events, update the task view, synchronize to shared accounts.

6.2 Set Task Reminder Function

Function ID: FR-14

Description: Users can set multiple reminders for tasks, including single, recurring, and intelligent prediction modes, and support various notification channels.

Input: Task ID, reminder type (single/recurring/intelligent prediction), time settings, notification channel selection.

Output: Update task reminder configuration, update the reminder timeline, synchronize to the calendar and mobile devices, generate reminder operation logs.

6.3 Modify Task Status Function

Function ID: FR-15

Description: Users can modify the task status and record the history of status changes and their impact scope.

Input: Task ID, new status (e.g., in progress/completed), status change explanation.

Output: Update task status, update the Gantt chart, adjust the reminder timeline, generate status modification logs.

6.4 Delete Task Function

Function ID: FR-16

Description: Users can delete tasks and disassociate them from emails, contacts, and reminders.

Input: Task ID, deletion method (permanent/recycle bin), permission verification result.

Output: Update task status, disassociate reminders, update storage quotas, generate deletion operation logs.

7. Permission and Account Management Function

7.1 Configure Fine-Grained Permissions Function

Function ID: FR-17

Description: Administrators can configure fine-grained permissions for shared accounts, including access levels, folder controls, and validity periods.

Input: Shared account ID, permission configuration (access level, folder ID, validity period).

Output: Update permission information in the permission table, refresh the access control list, generate permission change logs.

7.2 Approve Email Application Function

Function ID: FR-18

Description: Administrators can approve users' email applications, including verifying application information, checking naming conventions, and storage quotas.

Input: Email application information (user information, email type, storage quota), approval result (approved/rejected).

Output: Update email status, adjust storage quotas, generate approval logs, send notifications to applicants.

7.3 Delete Shared Account Function

Function ID: FR-19

Description: Administrators can delete shared accounts and disassociate them from emails, contacts, and archiving policies.

Input: Shared account ID, deletion method (immediate/delayed), permission verification result.

Output: Update shared account status, release storage space, synchronize to archiving policies, generate deletion logs.

8. Email Archiving and Policy Management Function

8.1 Set Archiving Policy Function

Function ID: FR-20

Description: Administrators can create or modify archiving policies, including retention periods, storage locations, encryption methods, and legal compliance requirements.

Input: Archiving policy name, applicable objects (folders/accounts/contact groups), retention rules, storage location, encryption configuration.

Output: Write archiving policies to the policy library, update email flow processing rules, generate policy impact reports, synchronize to the backup system.

8.2 Classify and Archive by Policy Function

Function ID: FR-21

Description: The system must automatically classify and archive emails based on archiving policies and update the email status and storage location.

Input: Email ID, archiving policy match results, storage location availability verification.

Output: Update email archiving status, update email flow processing rules, generate archiving operation logs, trigger backup verification.

8.3 Execute Server Archiving Function

Function ID: FR-22

Description: The system must perform server archiving operations for emails and ensure the integrity, encryption, and storage optimization of the archived data.

Input: List of email IDs, archiving storage location, archiving policy configuration.

Output: Update email status to archived, update email flow pointers, generate archiving reports, trigger backup verification.

8.4 Capture Email Flow Data Function

Function ID: FR-23

Description: The system must capture email flow data and record the sender, recipient, timestamp, and traffic characteristics.

Input: Email flow data packet, SMTP/IMAP protocol parsing results, email flow monitoring configuration.

Output: Write email flow data to the monitoring log, generate traffic analysis reports, update email flow processing rules.

8.5 Process Expired Emails Function

Function ID: FR-24

Description: The system must process expired emails according to predefined rules, including deletion or archiving, and generate processing records.

Input: List of email IDs, expiration time, archiving policy match results.

Output: Update email status, release storage space, update expiration processing records, generate archiving reports.

9. Data Backup and Recovery Function

9.1 Perform Full Backup Function

Function ID: FR-25

Description: Administrators can initiate full backup tasks, and the system must ensure the integrity, encryption, and storage synchronization of the backup data.

Input: Backup type (full), target storage location, encryption configuration, compression settings.

Output: Generate backup image, update backup logs, synchronize to the disaster recovery system, generate backup reports.

9.2 Restore Data to a Specific Time Point Function

Function ID: FR-26

Description: Administrators can select a time point for data recovery, and the system must ensure the integrity and consistency of the recovered data.

Input: Time point selection, recovery scope (emails/contacts/tasks), storage location verification.

Output: Restore data to the specified time point, update recovery logs, generate integrity verification reports, send recovery notifications.

9.3 View Backup Logs Function

Function ID: FR-27

Description: Administrators can view backup operation logs and perform multidimensional analysis and anomaly pattern detection.

Input: Time range, backup type, executor filtering criteria.

Output: Backup log query results, generate audit summaries, flag suspicious operations, trigger security responses.

10. System Monitoring and Security Audit Function

10.1 Email Traffic Monitoring Function

Function ID: FR-28

Description: The system must monitor email traffic in real-time and detect abnormal communication behaviors and threat characteristics.

Input: Email flow data packet, SMTP/IMAP protocol parsing results, traffic baseline configuration.

Output: Write email traffic data to the monitoring log, generate real-time dashboards, flag abnormal traffic, trigger security protection mechanisms.

10.2 Permission Change Audit Function

Function ID: FR-29

Description: The system must record permission change operations and ensure they comply with the principle of least privilege and compliance requirements.

Input: Permission change operations (add/remove/modify), executor identity, effective time.

Output: Update permission change logs, generate permission impact reports, trigger security policy assessments, synchronize to the audit system.

10.3 Expired Email Processing Audit Function

Function ID: FR-30

Description: The system must audit the processing records of expired emails and ensure they comply with compliance standards and storage policies.

Input: Expired email processing logs, compliance standard selection, audit time range.

Output: Generate compliance audit reports, flag abnormal processing records, trigger repair workflows, synchronize to the blockchain evidence system.

11. System Maintenance and Management Function

11.1 Assign Administrator Permissions Function

Function ID: FR-31

Description: Super administrators can assign management permissions, and the system must ensure the compliance and principle of least privilege of the permission configuration.

Input: Target user ID, management permission role, permission scope definition.

Output: Write permission configuration to the RBAC database, update the ACL list, trigger security policy re-evaluation, generate permission change logs.

11.2 Manage Permissions Function

Function ID: FR-32

Description: Super administrators can manage permission configurations, including adding/removing permissions and adjusting scopes, and ensure system synchronization.

Input: Permission management operations (add/remove/adjust), target user or role ID, permission scope definition.

Output: Update the permission matrix, generate version snapshots, refresh the ACL list, synchronize to related subsystems.

11.3 Verify Backup Integrity Function

Function ID: FR-33

Description: Administrators can verify the integrity of backups, and the system must ensure the availability and consistency of the backup data.

Input: Backup ID, verification mode (full/sample), storage location verification.

Output: Generate integrity verification reports, flag damaged data blocks, trigger repair processes, update backup health status.

11.4 Batch Archiving Processing Function

Function ID: FR-34

Description: Administrators can perform batch email archiving operations and ensure the correct application of archiving policies and storage optimization.

Input: Archiving policy ID, email filtering conditions (time/folder/contact group), storage location verification.

Output: Complete batch email archiving, update email flow pointers, generate archiving reports, trigger backup verification.

11.5 Mark Email Priority Function

Function ID: FR-35

Description: Users can set the priority of emails and trigger associated reminders and archiving policy evaluations.

Input: Email ID, priority level (urgent/high/normal/low), processing time settings.

Output: Update email priority status, refresh email list indicators, update archiving policies, generate operation logs.

12. System Compatibility and Extension Function

12.1 Email Formatting Function

Function ID: FR-36

Description: The system must support rich text formatting of emails and provide attachment management and format checks before sending.

Input: Email body, attachment list, format check rules.

Output: Formatted email content, update attachment metadata, generate format check logs.

12.2 System Recovery Function

Function ID: FR-37

Description: The system must provide flexible recovery capabilities from file-level to database-level and support data restoration based on time points.

Input: Recovery scope (emails/contacts/tasks), time point selection, storage location verification.

Output: Restore data to the target location, update recovery logs, generate integrity verification reports, send notifications to relevant parties.

12.3 Operation Record Audit Function

Function ID: FR-38

Description: The system must record all management operations and generate audit logs to ensure traceability of operations.

Input: Operation type (create/modify/delete), target object (emails/contacts/tasks), executor identity.

Output: Write operation logs to the database, generate version snapshots, synchronize to the audit system, update operator permissions.

13. User Interface and Interaction Function

13.1 Email Archiving Search Function

Function ID: FR-39

Description: Users can search archived emails and ensure decryption permissions and compliance filtering.

Input: Search criteria (time range, archiving date, encryption status), permission verification results.

Output: Archived email search result set, update archiving access logs, generate compliance reports, synchronize to the disaster recovery system.

13.2 Move Email to Folder Function

Function ID: FR-40

Description: Users can move emails to specified folders and ensure re-evaluation of permissions and archiving policies.

Input: List of email IDs, target folder ID, permission verification results.

Output: Update email storage paths, refresh folder lists, trigger archiving policy evaluations, generate operation audit logs.

13.3 Email Label Management Function

Function ID: FR-41

Description: Users can add or remove labels to/from emails and ensure the association of labels with archiving policies.

Input: List of email IDs, label name, color code, policy binding.

Output: Update email label status, refresh email list display, trigger archiving policy evaluations, generate label operation logs.

14. System Security and Compliance Function

14.1 Email Flow Capture and Monitoring Function

Function ID: FR-42

Description: The system must capture email flow data and record traffic monitoring logs to ensure data auditability.

Input: Email flow data packet, monitoring rules, storage location verification.

Output: Write traffic data to the monitoring log, generate monitoring alerts, update traffic statistics views, synchronize to the security analysis platform.

14.2 Email Flow Alert Handling Function

Function ID: FR-43

Description: The system must handle email flow alerts and ensure that alert events are traceable and responsive.

Input: Alert type (traffic anomaly/malicious attachment), timestamp, traffic characteristics.

Output: Record alert events, update monitoring logs, trigger security response processes, generate alert summary reports.

14.3 Email Flow Compliance Assessment Function

Function ID: FR-44

Description: The system must assess the compliance of email flows and ensure that email processing complies with laws and corporate policies.

Input: Email flow data packet, compliance standards (GDPR/HIPAA), policy match results.

Output: Compliance assessment report, flag non-compliant emails, trigger manual review processes, update archiving policies.

15. System Performance and Optimization Function

15.1 Email Flow Load Optimization Function

Function ID: FR-45

Description: The system must optimize the load of email flows to ensure processing efficiency under high load conditions.

Input: Email flow load data, optimization strategies (sharding/parallel), resource quota check.

Output: Complete email flow processing optimization, update load statistics, generate performance analysis reports, synchronize to the monitoring system.

15.2 Archiving Policy Health Assessment Function

Function ID: FR-46

Description: The system must assess the health of archiving policies and generate optimization suggestions.

Input: Archiving policy execution logs, storage space utilization, email processing efficiency.

Output: Policy health score, generate optimization suggestion list, flag policies for adjustment, update the policy management interface.