Functional Requirement

1.1 Email Sending Function

Function ID: FR-01

Description: After the user inputs the email content in the email editing interface, they can submit the email to the server for sending. The system needs to verify the recipient's address, attachment size, and the user's sending permissions. Once the verification is successful, the email is submitted to the SMTP server.

Input: Email content (subject, body, attachments), recipient's email address (manual input or selected from contacts/distribution groups), send time (immediate or scheduled).

Output: The email is successfully delivered to the recipient's server, the sending log is recorded in the system log entity, and the email draft is automatically saved to a folder (if sending fails).

1.2 Email Receiving Function

Function ID: FR-02

Description: The system periodically pulls new emails from the email server and performs basic verification (sender, email header integrity, email size), security scanning (virus detection, malicious link analysis), and finally stores the email in the inbox folder and generates a desktop notification.

Input: Email data from the email server (email header, body, attachments).

Output: New emails are stored in the inbox folder, the receiving log is updated to the backup log entity, and suspicious emails are moved to the quarantine area.

1.3 Email Formatting Function

Function ID: FR-03

Description: Users can format the email body in the email editing interface using rich text formatting, including font styles, paragraph formatting, table insertion, etc. The system needs to verify the format compatibility in real-time to ensure the email is displayed correctly on different clients.

Input: Email body content, formatting operations (font/paragraph/table/hyperlink).

Output: The formatted email content is saved to a folder, and the formatting operation log is recorded in the backup log entity.

1.4 Email Search Function

Function ID: FR-04

Description: Users can search for emails using advanced search functions based on keywords, time ranges, senders/recipients, attachment types, and other conditions. The system needs to verify search permissions and return a list of matching emails.

Input: Search criteria (keywords, time range, folder path, attachment type).

Output: A list of emails that meet the criteria, and the search log is recorded in the backup log entity.

1.5 Email Archiving Function

Function ID: FR-05

Description: Users or the system can migrate emails to the archive folder according to the archiving policy to free up storage space and meet compliance audit requirements. The system needs to perform pre-archiving verification and update the backup log and recovery log.

Input: Archiving trigger conditions (manual archiving, storage threshold, retention period), archiving policy (retention years, storage tier).

Output: Target emails are moved to the archive folder, and the archiving log is recorded in the backup log entity.

1.6 Email Deletion Function

Function ID: FR-06

Description: The system deletes expired emails and frees up storage space based on retention policies or administrator instructions. The system needs to ensure that the deletion operation complies with legal retention requirements and is recorded in the backup log and recovery log.

Input: Deletion trigger conditions (retention period, storage over-limit, compliance deletion), deletion mode (logical deletion, physical erasure).

Output: Target emails are deleted, storage space is freed, and the deletion log is recorded in the backup log entity.

1.7 Contact Creation Function

Function ID: FR-07

Description: Users can create new contacts in the address book module. The system needs to verify the email format, phone number format, and field completeness, and encrypt the contact information for storage.

Input: Contact information (name, email, phone, position).

Output: Contact entity is created, and the operation log is recorded in the backup log entity.

1.8 Contact Editing Function

Function ID: FR-08

Description: Users can edit existing contact information. The system needs to verify field formats and permissions, and save historical versions to the recovery log.

Input: Contact ID, modified fields (name, contact information, notes), permission verification.

Output: Contact information is updated, and the historical version is recorded in the recovery log entity.

1.9 Contact Deletion Function

Function ID: FR-09

Description: Users or administrators can delete contacts. The system needs to check whether they are referenced by other business entities and generate a deletion log.

Input: Contact ID, deletion scope (delete only the current contact, synchronously remove associated distribution group membership).

Output: The contact is removed from the address book, associated references are updated, and the deletion log is recorded in the backup log entity.

1.10 Contact Search Function

Function ID: FR-10

Description: Users can search for contacts in the address book using advanced search functions. The system needs to verify permissions and return a sorted list of contacts.

Input: Search criteria (name, email, department, distribution group, last contact time).

Output: A list of matching contacts, and the search log is recorded in the backup log entity.

1.11 Distribution Group Creation Function

Function ID: FR-11

Description: Users can create new distribution groups in the address book module. The system needs to verify the uniqueness of the group name and the validity of member email addresses, and generate a unique identifier for the distribution group.

Input: Distribution group name, group type (static, dynamic), member list, permission settings.

Output: Distribution group entity is created, and the operation log is recorded in the backup log entity.

1.12 Distribution Group Member Management Function

Function ID: FR-12

Description: Users or administrators can manage distribution group members, including adding, removing, and adjusting permissions. The system needs to verify permissions and synchronize updates to the distribution group and related entities.

Input: Distribution group ID, member operations (add/remove/permission adjustment), permission verification.

Output: Distribution group member relationships are updated, and the operation log is recorded in the backup log entity.

1.13 Distribution Group Deletion Function

Function ID: FR-13

Description: Users or administrators can delete distribution groups. The system needs to check for dependencies and generate a deletion log.

Input: Distribution group ID, deletion mode (logical deletion, physical deletion), permission verification.

Output: The distribution group entity is deleted, associated member relationships are dissolved, and the deletion log is recorded in the backup log entity.

1.14 Calendar Event Creation Function

Function ID: FR-14

Description: Users can create calendar events in the calendar module. The system needs to verify the time format and participant status, and send iCalendar invitations.

Input: Event subject, time range, recurrence rule, participant list, reminder method.

Output: Calendar event entity is created, iCalendar invitation is sent, and the operation log is recorded in the backup log entity.

1.15 Calendar Event Modification Function

Function ID: FR-15

Description: Users or administrators can modify existing calendar events. The system needs to verify time conflicts and participant availability, and generate a new version.

Input: Event ID, modified fields (time range, participants, reminder method), permission verification.

Output: Calendar event information is updated, change notifications are sent, and the operation log is recorded in the backup log entity.

1.16 Calendar Event Reminder Function

Function ID: FR-16

Description: The system reminds users of upcoming calendar events according to the set reminders and notifies them through email, pop-up windows, SMS, and other channels.

Input: Event ID, reminder time, notification channel.

Output: Reminder notifications are successfully delivered, and the operation log is recorded in the backup log entity.

1.17 Calendar Event Viewing Function

Function ID: FR-17

Description: Users can view a list of calendar events in the calendar view. The system needs to verify permissions and provide filtering and sorting functions.

Input: Time range, filter criteria (completion status, type), permission verification.

Output: A list of calendar events that meet the criteria, and the view log is recorded in the backup log entity.

1.18 Folder Creation Function

Function ID: FR-18

Description: Users can create new folders in the email management interface. The system needs to verify the uniqueness of the folder name and storage quota, and generate a unique identifier.

Input: Folder name, parent folder ID, permission settings, automatic categorization rules.

Output: Folder entity is created, and the operation log is recorded in the backup log entity.

1.19 Folder Renaming Function

Function ID: FR-19

Description: Users can rename existing folders. The system needs to verify permissions and synchronize updates to the index and related rules.

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

Output: Folder name is updated, and the operation log is recorded in the backup log entity.

1.20 Folder Moving Function

Function ID: FR-20

Description: Users can move folders to a specified path. The system needs to verify permissions and ensure data integrity.

Input: Source folder ID, target path, permission verification.

Output: Folder migration is completed, and the operation log is recorded in the backup log entity.

1.21 Folder Deletion Function

Function ID: FR-21

Description: Users or administrators can delete folders. The system needs to check if they contain protected emails and generate a deletion log.

Input: Folder ID, deletion mode (permanent deletion, move to trash), permission verification.

Output: The folder entity is deleted, storage space is freed, and the deletion log is recorded in the backup log entity.

1.22 Email Account Creation Function

Function ID: FR-22

Description: Administrators can create email accounts in the account management interface. The system needs to verify the validity of the domain name and the uniqueness of the username, and allocate storage quotas.

Input: Username, domain name, storage quota, initial password, permission settings.

Output: Email account entity is created, and the operation log is recorded in the backup log entity.

1.23 Email Account Deactivation Function

Function ID: FR-23

Description: Administrators can deactivate non-compliant email accounts. The system needs to verify the account status and freeze related sessions and permissions.

Input: Email account ID, deactivation reason, permission verification.

Output: The email account status is updated to "deactivated," and the operation log is recorded in the backup log entity.

1.24 Email Account Cancellation Function

Function ID: FR-24

Description: Users can apply to cancel their email accounts. The system needs to verify that there are no ongoing business dependencies and securely clean up data.

Input: Email account ID, cancellation confirmation code, permission verification.

Output: The email account status is updated to "cancelled," data cleanup is completed, and the operation log is recorded in the backup log entity.

1.25 Email Account Password Reset Function

Function ID: FR-25

Description: Users can reset their email account passwords. The system needs to verify multi-factor authentication and update the password hash.

Input: Email address, verification code, new password, permission verification.

Output: The email account password is updated, and the operation log is recorded in the backup log entity.

1.26 Shared Account Creation Function

Function ID: FR-26

Description: Administrators can create shared accounts in the shared account management interface. The system needs to verify permissions and allocate storage quotas.

Input: Shared account name, creator ID, member list, validity period, permission settings.

Output: Shared account entity is created, and the operation log is recorded in the backup log entity.

1.27 Shared Account Permission Management Function

Function ID: FR-27

Description: Administrators can manage access permissions for shared accounts. The system needs to verify the permission chain and synchronize updates to the ACL.

Input: Shared account ID, permission changes (role, validity period, operation type), permission verification.

Output: Shared account permissions are updated, and the operation log is recorded in the backup log entity.

1.28 Email Attachment Management Function

Function ID: FR-28

Description: Users can upload, delete, and rename email attachments. The system needs to verify the attachment size and type, and perform security scanning.

Input: Attachment file, email ID, operation type (upload/delete/rename), permission verification.

Output: Attachment operations are completed, and the operation log is recorded in the backup log entity.

1.29 Attachment Virus Scanning Function

Function ID: FR-29

Description: The system needs to automatically scan attachments for viruses during email receipt or sending to ensure email security.

Input: Attachment file, email ID, scanning engine configuration.

Output: The attachment status is marked as "safe" or "quarantined," and the log is recorded in the recovery log entity.

1.30 Dynamic Distribution Group Rule Configuration Function

Function ID: FR-30

Description: Administrators can configure rules for dynamic distribution groups. The system needs to verify the rule syntax and synchronize updates to the member list.

Input: Distribution group ID, dynamic rules (query conditions, member expansion rules), permission verification.

Output: Distribution group configuration is updated, member list is dynamically adjusted, and the operation log is recorded in the backup log entity.

1.31 Dynamic Update of Distribution Group Members Function

Function ID: FR-31

Description: The system needs to automatically update distribution group members based on dynamic rules to ensure that the distribution group information is up-to-date.

Input: Dynamic rules, distribution group ID, time trigger.

Output: Distribution group members are updated, and the operation log is recorded in the backup log entity.

1.32 Server Health Monitoring Function

Function ID: FR-32

Description: The system needs to monitor the health status of the email server, including load rate, SSL certificate validity, etc., and record logs.

Input: Email server ID, monitoring indicators (load rate, certificate fingerprint, queue depth).

Output: Server health status is updated, and the log is recorded in the audit log entity.

1.33 Backup File Generation Function

Function ID: FR-33

Description: The system needs to generate encrypted backup files according to the backup policy and record them in the backup log.

Input: Backup policy ID, data entity (emails, contacts, calendar events), encryption algorithm, compression format.

Output: Backup file is generated, and the operation log is recorded in the backup log entity.

1.34 Recovery Log Recording Function

Function ID: FR-34

Description: The system needs to record all recovery operations, including the time point, operator, and recovery scope, and ensure that the log is tamper-proof.

Input: Recovery operation type, operator ID, recovery scope, recovery time point.

Output: Recovery log entity is created, and the operation log is recorded in the backup log entity.

1.35 Point-in-Time Recovery Function

Function ID: FR-35

Description: The system needs to support point-in-time recovery of email data, ensure data consistency, and record recovery logs.

Input: Time point ID, recovery scope (user/department/full database), permission verification.

Output: Data is recovered to the specified time point, and the recovery log is recorded in the backup log entity.

1.36 Audit Log Recording Function

Function ID: FR-36

Description: The system needs to record audit logs for all critical operations, including operation type, target object, and field change details, to ensure compliance.

Input: Operation type, target object type, original value/new value comparison, permission verification.

Output: Audit log entity is created, and the operation log is recorded in the backup log entity.

1.37 Backup Integrity Verification Function

Function ID: FR-37

Description: The system needs to perform integrity verification on backup data to ensure that backup files are not damaged.

Input: Backup ID, verification algorithm (SHA-256), verification frequency.

Output: Integrity verification result, log recorded in the recovery log entity.

1.38 Recovery Integrity Verification Function

Function ID: FR-38

Description: The system needs to verify the integrity of recovered data during the data recovery process to ensure data consistency.

Input: Recovery ID, verification algorithm (SHA-256), recovery time point.

Output: Integrity verification result, log recorded in the recovery log entity.

1.39 Email Server Parameter Configuration Function

Function ID: FR-39

Description: Administrators can configure parameters for the email server, including SMTP/IMAP protocol settings. The system needs to verify the parameter format and update the configuration file.

Input: Server ID, parameter type (SMTP/IMAP), configuration value, permission verification.

Output: Server configuration is updated, and the operation log is recorded in the backup log entity.

1.40 Email Server Load Balancing Function

Function ID: FR-40

Description: The system needs to dynamically allocate email processing tasks based on the load rate of the email server to ensure high availability of email transmission.

Input: Email entity, server cluster status (load rate, availability).

Output: Email is routed to an available server node, and the log is recorded in the email server entity.

1.41 Archiving Policy Definition Function

Function ID: FR-41

Description: Administrators can define email archiving policies. The system needs to verify retention years and storage tiers, and synchronize updates to the email status.

Input: Policy ID, classification rules, retention years, storage tier, permission verification.

Output: Archiving policy entity is created, and the operation log is recorded in the backup log entity.

1.42 Archiving Policy Application Function

Function ID: FR-42

Description: The system needs to automatically tag emails based on the archiving policy and trigger archiving operations to ensure data compliance.

Input: Archiving policy ID, email entity, timestamp.

Output: Email archiving status is updated, and the operation log is recorded in the backup log entity.

1.43 Email Flow Capture Function

Function ID: FR-43

Description: The system needs to capture and record the sending, receiving, and forwarding paths of email flows to ensure the integrity of email auditing.

Input: Email ID, operation type (send/receive/forward), timestamp.

Output: Email flow path is recorded in the audit log entity, and the operation log is recorded in the backup log entity.

1.44 Policy-Based Classification and Archiving Function

Function ID: FR-44

Description: The system needs to archive emails based on classification rules (keywords, sender, time period) to ensure data classification storage.

Input: Email entity, archiving policy ID, classification rules.

Output: Email is archived to the specified folder, and the operation log is recorded in the backup log entity.

1.45 Expiration Email Processing Function

Function ID: FR-45

Description: The system needs to process expired emails based on retention policies, including deletion or archiving, to ensure data lifecycle compliance.

Input: Email ID, retention policy, processing mode (delete/archive).

Output: Email status is updated, and the operation log is recorded in the backup log entity.

1.46 Email Backup Function

Function ID: FR-46

Description: The system needs to back up email data and record backup logs to ensure data recoverability.

Input: Email entity, backup policy ID, timestamp, permission verification.

Output: Email backup is successful, and the operation log is recorded in the backup log entity.

1.47 Data Recovery Function

Function ID: FR-47

Description: Administrators can recover specified emails or data entities based on recovery logs. The system needs to ensure the integrity of the recovered data.

Input: Recovery ID, recovery scope (email, folder, distribution group), time point, permission verification.

Output: Data recovery is successful, and the operation log is recorded in the recovery log entity.

1.48 Recovery Log Query Function

Function ID: FR-48

Description: Administrators can query recovery logs to understand the complete records of system recovery operations. The system needs to verify permissions and return results.

Input: Query conditions (time range, operation type, recovery scope), permission verification.

Output: Recovery log query results, operation log recorded in the backup log entity.

1.49 Backup Log Query Function

Function ID: FR-49

Description: Administrators can query backup logs to understand the complete records of system backup operations. The system needs to verify permissions and return results.

Input: Query conditions (time range, backup type, storage location), permission verification.

Output: Backup log query results, operation log recorded in the backup log entity.

1.50 Audit Log Query Function

Function ID: FR-50

Description: Administrators can query audit logs to understand the complete records of system operations. The system needs to verify permissions and return results.

Input: Query conditions (time range, operation type, target object type), permission verification.

Output: Audit log query results, operation log recorded in the backup log entity.