



Mail Server Solution

Website
www.sharetech.com.tw/en-us

✉ Sales Info
sales@sharetech.com.tw

✉ Tech Support
help@sharetech.com.tw



[Security × Business Continuity] How to Handle Departing Employee Email Accounts Properly

In enterprise IT management, account management is easily overlooked, especially when employees leave. Simply deleting their email accounts risks business disruption, but keeping them active opens security risks.

Here are ShareTech's 4 practices for managing departed employee accounts—ensuring both [business continuity and information security](#).

1. Enable Auto-Forwarding or Auto-Reply

After an employee leaves, external contacts may still email their old address. Without proper handling, those messages will never get replied—causing missed opportunities and broken client relationships.

What to do: Set up [auto-forwarding](#) to the new responsible person's mailbox so no email is left behind. It is better if you also set [auto-reply](#) messages like:

"Hello, I have resigned. [xxx@company.com](#) will take over my job and reply to you!"

This ensures smooth communication and preserves trust and efficiency.

2. Disable the Account to Prevent Unauthorized Access

Letting a former employee's account remain active is a data breach waiting to happen. But deleting it too fast risks losing important info.

What to do: [Disable the account](#) to reject logins, while optionally [keeping it able to receive emails](#). You can also set an [automatic deletion period](#)—such as 90 or 180 days—based on company policy to allow a buffer for data handling.

This strikes a balance between security and flexibility.



3. Remove from Shared Address Books and Group Accounts

Seeing an ex-employee listed in the company address book can lead to [misdirected emails](#) or the mistaken belief that they are still on staff, causing confusion.

If the account remains in group accounts and has special system permissions, it may result in [unauthorized data access](#).

What to do: Remove the user from the shared address book and group accounts. This prevents unnecessary mail delivery and reduces access risks.

4. Back Up Emails to Prevent Disputes or Loss

In legal or business disputes, missing email records is a nightmare.

What to do: Enable the mail recorder to automatically log all inbound and outbound emails. You can set exception rules to exclude certain emails from logging. Preserve all emails from the departed user or forward them to the successor's mailbox to ensure records are available for legal, audit, or customer inquiry purposes.

Even better: Use a [ShareTech Mail Archive](#) server to offload backup and email query workloads from the ShareTech Mail Server and ensure greater security with [encrypted archived data](#).

With one setup, you ensure security, compliance, and dispute evidence—all covered!

Conclusion: Managing departing accounts is a professional responsibility.

Handling departing accounts isn't just a minor admin task—it directly affects your business continuity, transparency, and security posture.

What to do: Build it into SOP and deploy a [ShareTech Mail Server](#) for automated forwarding, replying, recording, and account disabling.

An account isn't "just deleted"—it's [your commitment to cybersecurity and business continuity](#). Want to learn more or try our email management tools? Contact us at sales@sharetech.com.tw!