Implement Employee Off-Boarding and Email Retention Solutions to Protect Your Organization

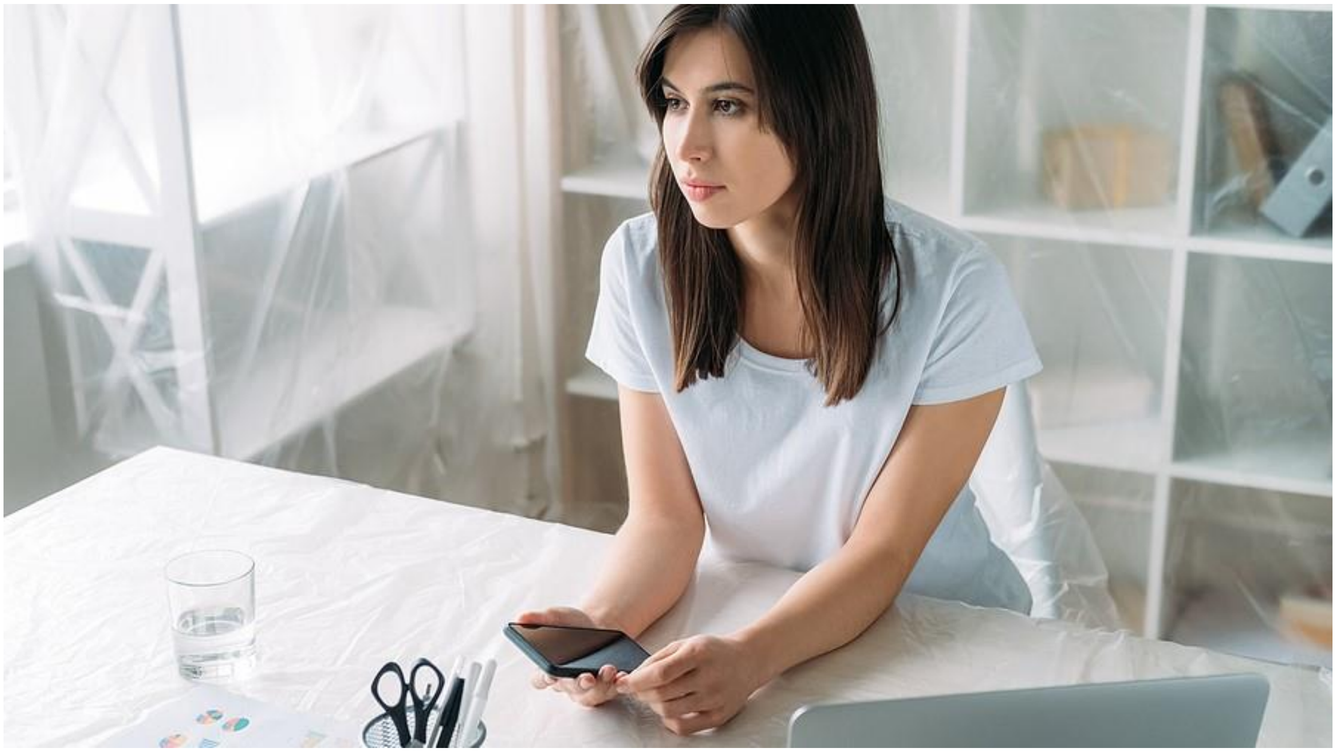
When employees leave the company, organizations must determine how to deal with departing users' accounts to provide protection while limiting company liability. Microsoft 365 and other applications offer several options for addressing employee off-boarding and email retention. The scenarios in this post will help you determine the best solution for your company.

Start by Defining a Retention Policy

A departing employee leaves behind a digital footprint, including email accounts and other data. Organizations need the ability to review and keep relevant content from ex-employees. At the same time, they need to balance information access with data privacy law requirements and potential eDiscovery needs.

Before determining the best off-boarding solution, the organization should attempt to define a data retention policy, particularly for email. Defining this policy will assist IT in deploying local systems policies and licensing levels. It will also ultimately define what data will be available in any external data request.

Keep in mind that Microsoft 365 ties data retention and access to licensing. For instance, full retention of data, including allowing access by other individuals, requires a minimum Microsoft 365 E3 plan. This enterprise plan requires an annual commitment at twenty dollars per user per month. Alternatively, organizations may consider an external, third-party solution.



Microsoft 365 Off-Boarding and Email Retention Solutions

Microsoft 365 offers several solutions for determining email retention for departing employees. For instance, the organization may choose to retain the mailbox for the ex-employee and grant delegate access to another employee, such as a manager. This delivers a quick and easy solution. However, the organization will still have to pay for the user license.

Alternatively, the email administrator can easily convert the ex-employee mailbox to a shared mailbox. This provides access to the data without the expense of maintaining a licensed account.

However, while shared mailboxes facilitate sharing of information, they do not offer any data protection. Because shared mailboxes do not have the same retention and data preservation policies as regular, licensed accounts, data in them can be irrevocably deleted. Additionally, shared mailboxes can still receive emails and may generate costs for SPAM filtering.

As a third option, organizations may place data in a retired mailbox on litigation hold or under a retention policy. This preserves the data. However, unless the account is given a license and assigned delegate access, only eDiscovery and compliance managers can search for the data.

Consider the following typical off-boarding scenarios with Microsoft 365:

- **Non-essential worker** – These include seasonal/term workers that do not typically use email for day-to-day business. For these workers, first remove the worker's access to the email account. Then delete the account. Unless the data has been backed up, it will be irrevocably deleted after 30 days.
- **Essential worker** – These include standard employees involved in day-to-day business over email. For essential workers, first disable the email account. Then assign data access to a

manager for 90 days and create an auto-response rule. After 90 days, remove the account and delete the data.

- **Sensitive worker** – These include privileged employees or decision makers with access to important data. In the case of sensitive workers, first disable the email account and put it into data retention or litigation hold. Remove the license. The data will be accessible through eDiscovery indefinitely.

Third-Party Solutions

In some cases, organizations may find it more practical to look at third-party solutions, such as external archives. These solutions preserve data for eDiscovery while making that data also available for end users to review, albeit in a more restrictive manner. This option offers several key benefits.

External archives provide independent data storage, allowing retention of data regardless of the source license level. Additionally, archiving reduces the licensing cost for sharing, retention, and eDiscovery. Finally, unlike a backup, archiving preserves the ability to search and export data for access and recovery, with full auditing of all data access.

In a typical off-boarding scenario for essential and sensitive workers, email administrators first disable the email account. They then export contents of the account to a third-party archive and assign access to a manager. Finally, they delete the Microsoft 365 account and assign a retention policy to archive data. Managers and auditors can then search the archived data.

Email and Compliance Experts at Your Service

The email migration experts at Messaging Architects bring deep experience in both Microsoft 365 and third-party solutions, as well as data compliance. Our consultants will help you determine and implement the right off-boarding and email retention solution for your business.