White Paper

# Archive2Azure™

## Office 365 Tips for Protecting Data for Departed Employees

From **Archive360™**

ARCHIVE360

POINT. CLICK. MIGRATE. STORE.

## Introduction

It is a fact of life for every organization that employees leave the company. Whether it is the decision of the employee or the employer, the impact on IT is the same. The employee's access to company networks must be removed and the employee's data must be preserved. To illustrate, the Ponemon Institute[1], a Tucson based research group, conducted interviews with 945 adults who were laid off, fired or changed jobs in the last year. The results were very interesting and highlight the magnitude of this important issue.

- Nearly 60 percent of employees who depart a job steal company data.
- Seventy-nine percent of those who admitted to taking data said they did so despite knowing that their former employer did not permit them to take internal company information.
- Sixty-five percent of those who took data from their former employer grabbed e-mail lists.
- Roughly sixty-seven percent of those who acknowledged taking company data said they did so in order to leverage a new job.
- Twenty-four percent of responders said they still had access to their employer's computer network after they departed.

These statistics reveal just how important it is for company management to understand the problem and develop processes to manage employee departures properly. The first step is to develop a departing employee's plan and process. A comprehensive plan includes many different departments including IT, HR, and Legal. In this paper we will focus on the technical issues facing IT with respect to Microsoft Office 365 data preservation. To start off with, we will examine employee behavior and how the IT department can better prepare itself to manage this critical issue.

## Signs of unusual employee behavior

When the employee decides to quickly depart the company, it is very difficult for IT to take preventive measures to protect corporate information. To help, there are certain signs that you can look for that may indicate when an employee is preparing to leave the company:

**Top Reasons Employees think it is Ok to take Company Information:**

- Sharing the information does not harm the company
- The company has a policy that is not strictly enforced.
- Business information is generally available and not secured.

- The employee is copying large numbers of documents and files to USB drives or the cloud
- The employee is sending documents via email large attachments to personal email account (e.g. Gmail)
- The employee is accessing the building after typical business hours
- The employee is using the company email system to communicate with competitors
- The employee is deleting large numbers of documents or records on CRM, file share, laptop, etc.
- Multiple employees are leaving the same department at the same time

The challenge you face when an employee departs un-expectantly, should not be underestimated. Take for example a simple flash drive that sells for $50 at the local electronic store. Assuming 1GB can hold up to 60,000 pages of content, then a 256GB flash drive can hold over 15M documents, or 6,000 boxes of documents. Even a single 10MB email attachment can hold on average over 600 documents and files.

[1] *Research conducted by Ponemon Institute, 2009.* http://www.ponemon.org/

## Common target data

Employees who depart the company typically are interested in taking job function related information. For employees in sales and marketing, customer contact information, price lists, and product information is highly popular. For employees in engineering, product designs, trade secrets, or other intellectual property are favored. Below is a sample list of information that is favored by employees when they depart the company:

- Customer names and contact information
- Price lists and costing information
- Internal product roadmaps
- Competitive information
- Internal product presentations
- 3rd-party industry research reports
- CRM and Sales related data (opportunities, accounts, contracts)
- Employee contact information for recruiting
- Engineering designs, trade secrets or other intellectual property
- Investment, accounting (stock, profit/loss) and credit data

## Data protection challenges

Ultimately the challenge of protecting company information is not a technical problem as much as a people issue. Employees with good intentions are unlikely to steal company information; while employees with questionable intentions can easily steal large amounts of information no matter what you do. Nevertheless, there are important technical steps you can take to safeguard company information. Below is a partial a list of actions and precautions you can take to safeguard company information before (and after) an employee departs the company.

- Restrict access to highly confidential information
- Insert clear confidentiality provisions in employment contracts and remind them of the provisions during the exit interview
- Develop policies on proper use of email/computers/mobile devices
- Adopt policies to audit and enforce all policies to deter misbehavior
- Conduct employee training on policies
- During exit interview ask questions about future plans/employment to determine potential risk
- Disable all employee accounts, email, remote access, key cards, etc. on employee exit
- Keep internal access to employee accounts for possible audit or investigation
- Copy and safely store employee electronic files, documents in a central, secure repository in case of later litigation
- Wipe personal devices used for work for example of company email accounts as permitted by company policy

## Protecting Office 365 Cloud Services

If you are like the majority of medium and large enterprise companies, you are probably using Microsoft Office 365 cloud services. Office 365 is a complete communication and collaboration platform that provides essential email and calendaring services as well as valuable user productivity applications for file sharing, instant messaging and real-time collaboration. The shear breadth of data that is created and managed by Office 365 is a major challenge to IT professionals. To complicate matters further, being a cloud-based service makes it very difficult to prevent unwanted dissemination of sensitive company information outside of the enterprise.

If your organization is using Office 365, you should have processes in place to ensure proper data handling when an employee departs. Your actions can be broken down into two parts: the first to control access to information, and the second to preserve the information itself. Generally speaking, user access is centrally managed in Microsoft Active Directory (AD), but there are certain unrecoverable consequences when you delete a user account. End-user data and what happens to it when an employee leaves should be accounted for including being backed up, but there are additional steps you should take to change access to departing user data including ensuring its availability to co-workers and the departed user's manager.[2]

Checklist of high level actions needed to manage departing users Office 365 accounts and data:

- Immediately block user access to Office 365 data and Exchange Online
- Preserve the contents of the user's mailbox (litigation hold)
- Wipe and block the user's mobile device if it is company issued, otherwise remotely wipe all company accounts from employee's personal device
- (Optional) Forward the user's email to another employee such as their manager
- Remove the user's Office 365 license so you can assign it to a new employee
- Delete the former employee's user account

In the next section we will examine each action in the context of the Office 365 component (e.g. Active Directory, Exchange, OneDrive and SharePoint) that may/is impacted.

## Tips for blocking user access when needed

The first step with Office 365 is to disable user account access. This is accomplished in the Office 365 Admin Center. Here you navigate to the user account and change the "Sign-in status" to "blocked". This ensures that the departed employee cannot access his or her Office 365 account at all. If the use has an Exchange email account, you block email access in the Exchange Admin Center (EAC). Here you can disable email connectivity, disable OWA for devices and disable Exchange ActiveSync.

After you have removed the departed user's access to Office 365, you need to decide who should have access to the work data. In most cases, the obvious choice is the departed user's manager. The manager surely wants to receive emails that would normally go to the departed employee, so he can respond and provide continuity during the transition. A co-worker may also need access for the same reason – you do not want email sent to the departed employee to go unanswered. Using the same Office 365 Admin Center, you can forward all the departed employee's email to a new user and/or you can share the departed employee's mailbox with a new user.

Next, it is important to decide how long you want to grant access to the manager or co-worker. The reason is that as long as another user has access to the departed user's mailbox, the departed user's Office 365 license is still in use. The length of time you keep the Office 365 account active depends on the organization. Do you work for a large college where you routinely disable thousands of email accounts every year? Or is the need to disable an account an infrequent occurrence? Depending on your organization, you can decide to keep disabled accounts around for weeks, months or years.

## Exchange Online tips for preserving email data for legal reasons

Before you remove user data, you must determine if the departed user is part of an active litigation

[2] https://support.office.com/en-us/article/Remove-a-former-employee-from-Office-365-44d96212-4d90-4027-9aa9-a95eddb367d1

matter, or if they could be involved in future litigation. Depending on the type of employee (e.g. regular, contractor, manager, executive) and the user's access to confidential information, you may be required to preserve all mailbox contents for prolonged periods of time. This is done by placing the mailbox on "Litigation Hold" or "In-Place Hold" using the Exchange Online Admin Center. The legal hold can be set to last for a specific period of time or indefinitely. A benefit of using Office 365 is that inactive mailboxes are preserved in Office 365 without incurring any license or storage fees. For legal discovery, active and inactive mailboxes can be searched by eDiscovery Center, a component of Office 365 E3 and E5 licenses.

## OneDrive tips for preserving file data

Preserving a departed user's OneDrive data is not as straight-forward. To start with, the retention period for cleanup of OneDrive begins when the user's Office 365 license is removed. No other action will cause the cleanup process to occur so be very careful when you remove a license or delete a user account from Office 365. When the cleanup job runs, an email notification is sent to the user's manager stating that access has been granted to the manager and that the content will be irretrievably deleted after 30 days.

To preserve the departing user's valuable OneDrive data, the manager can access the departed user's OneDrive account via the URL provided in the notification email. The manager ***can manually copy or move files one-at-a-time via the web browser interface.*** A better solution is to configure the Explorer sync client, then you have access to the files via Explorer and can copy files in bulk where you want. Optionally, there are third-party migration tools to migrate data in bulk.

## SharePoint tips for preserving file data

The process SharePoint follows to clean up "My Site" data is very similar to OneDrive. Once the user Office 365 account is deleted, the cleanup timer job runs, and the user profile is marked for deletion. The profile will be preserved in the database in a deleted state for 30 days. The manager receives an email message that states that the My Site for the departed user will be removed in 30 days and that access to the site is granted to the manager for that time period. During the 30-day period, the manager can access the departed user's files and move files to an alternate location for preservation. Using the SharePoint interface, ***the manager can download or remove files and documents one-at-a-time.*** Optionally, there are third-party migration tools to migrate data in bulk.

## Skype for Business tips for preserving data

User data in Skype is preserved in the user mailbox when a Litigation Hold or In-Place Discovery Hold has been initiated. From this point in time forward, all Skype communication is preserved and can be searched for eDiscovery. When an employee departs, unless a Litigation Hold or In-Place Discovery Hold has been in place, there is no way to preserve data in Skype. Optionally, there are third-party archiving tools to preserve Skype data in bulk.

## My Documents tips for preserving file data

And finally, it is important to preserve files and documents that are stored on the departed user's desktop (or laptop). Depending on the Office 365 subscription, the My Documents folder can contain additional Office 365 data from for example OneNote or other applications. Common practice is to assume control of the user's desktop the moment he or she leaves the company. This is often done by the hiring manager or HR personnel. With the desktop in possession, files and documents can be copied or moved to a new 'archive' location. Potentially, there are additional actions to take depending on the applications provided to each employee.

A best practice is to design a 'cleanup' process so data is copied from the user device and stored in a 'archive' location that facilitates search and discovery. Practices that are not recommended include removing the hard drive and locking it in a file cabinet or relying on the last backup and erasing or wiping the disk drive completely. The reason is future access. Both practices result in a large amount of data improperly stored and difficult to access. Should future legal discovery involve the departed user, it will require a large and expensive effort to restore a hard disk or search backup tapes.

## Final thoughts

As you design your process for protecting Office 365 for departing employees, there are a few important decisions for you to make. First, assuming that you want to re-use the Office 365 license in a reasonable amount of time (e.g. 30 days); you will need to remove the Office 365 license and delete the user account. Keep in mind that after 30 days, the entire Office 365 account and all of its data will be removed forever.

You can save the user's mailbox data easily; a highly recommended process especially if the user is part of a litigation matter or could be part of future litigation. Talk to your legal department and get written instructions, especially if they recommend deletion without preservation. To preserve a mailbox, put the user's mailbox on Litigation Hold using the Exchange Admin Center. This releases the Office 365 license and preserves the mailbox indefinitely or for a period of time you specify.

However, the OneDrive, OneNote, Skype, Yammer or SharePoint data is another matter. This data has to be preserved manually, if you decide to preserve it at all. At the end of 30 days it will all be deleted.

A couple of potentially major issues remain for managing and protecting data for departing employees. First, when data is copied/moved/removed from Office 365 after deletion of a user account, what if any issues do you need to consider around chain of custody reporting? Can you provide a report that documents what was copied/moved/deleted, when and by whom? This information is very critical for legal and compliance purposes.

Second, what to do with the departed user's laptop or desktop? Is your plan to re-image the disk drive after a specific period of time or, save it in a locked file cabinet incase a future wrongful termination lawsuit arises? Do you have a process to manually copy all the user's My Documents folders to a secure file share location? These questions are important to consider as they directly affect your time, productivity, and possible legal responsibilities.

## Archive2Azure

Archive2Azure uniquely offers a "one-click" solution to preserve a complete Office 365 account for a departed employee and it provides full chain of custody for legal and compliance. Archive2Azure can also migrate data from a user laptop or desktop with FastCollect. Admins will love the ability to quickly preserve a complete Office 365 account and release the license without concern for future needs. (e.g. future legal search, file restore, full account restores, etc.)

Archive2Azure is the industry's first cloud-based compliance storage solution that works seamlessly with Microsoft Office 365 and Microsoft Azure to preserve, protect, manage, and make available departed employee data. With easy access and infinite scalability, Archive2Azure delivers long-term retention of unstructured grey data including email and files for departed employees.

**Archive for Departed Employees:** Migrate and store all email and file data, for departed employees in a legally defensible and cost-effective manner to the low-cost Azure platform.

**Compliance Storage:** Archive2Azure stores archive content in original format and provides flexible, fast and forensically sound search results. Chain of custody context and data fidelity is fully maintained.

**On-Demand Indexing:** Incur index related compute and storage costs only when needed and in the manner you choose. Create custom index templates and target the data subsets you want to search.

**Native eDiscovery:** Case management, first-pass culling, tagging, review, and legal production is standard. Integrated Power BI offers a scalable eDiscovery engine with integrated analytics.

**Cost-Effective:** Based on affordable Azure 'cool' storage infrastructure, Archive2Azure is offered as a pay-as-you-go pricing model with no startup or cancellation fees.

## Conclusion

Every organization faces the challenge of protecting valuable company information when employees depart the company. With the rapid adoption of the cloud-based Office 365 platform, IT organizations face new challenges dealing with information protection for Exchange Online, OneDrive, SharePoint Online and the other applications provided as part of the Office 365 solution. In this paper we reviewed the challenge of protecting company information for departed employees and presented tips specific to Microsoft Office 365. By adhering to these technical tips combined with other best practices, organizations can go a long way in protecting valuable company information for departed employees.

## About Archive360

Archive360™ is the market leader in email archive migration software, successfully migrating more than 12 petabytes of data for more than 500 organizations worldwide since 2012. The company's flagship product, Archive2Anywhere™, is the only solution in the market purpose-built to deliver consistently fast, trouble-free, predictable archive migrations, with verifiable data fidelity and defensible chain of custody reporting. Archive360's newly released Archive2Azure™ solution is the industry's first regulatory compliance and long term grey data storage solution based on the Microsoft Azure platform. Archive360 is a global organization and delivers its solutions through a network of specialist partners. Archive360 is a Microsoft Cloud Solution Provider and the Archive2Azure solution is Microsoft Azure Certified. To learn more about Archive2Azure and the entire Archive2Anywhere platform contact Archive360 Sales.