Why You Need to Back Up Office 365

https://campus.barracuda.com/doc/78153951/

According to a January 2013 survey by Aberdeen Group, the number one cause of data loss in a SaaS deployment, such as Microsoft Office 365, is accidental data deletion. In fact, about 70 percent of all lost data is due to either accidental or malicious deletion of data by end-users. Other ways that data can be lost include misconfiguration, client sync issues, and most recently the widespread presence of malware and ransomware, which can render data unusable.

Microsoft's primary focus within Office 365 is ensuring that service and data availability are not disrupted. While Microsoft does a great job of reducing the risk of downtime, this does not reduce the risk of data loss. In fact, Microsoft's options for data recovery are quite limited, but they do provide some basic safety measures.

Use of Recycle Bins and Retention

Recently deleted content from Exchange Online, OneDrive for Business, and SharePoint Online is not deleted immediately. Instead, the deleted content goes through a set of Recycle Bins, each with their own retention policies, before it is deleted permanently. The Recycle Bins act as a safety net for deleted content. While data can be recovered from these Recycle Bins, the retention for each is limited and once the data is out of retention, the data is gone forever.

Table 1. Recycle Bins and Retention.

Microsoft Solution	Recovery Feature	Maximum Retention Period
SharePoint Online	Site Recycle Bin Second Stage Recycle Bin	93 days 93 days
Exchange Online	Deleted Items Recoverable Items	No maximum (configurable)(1) Up to 30 days(2)
OneDrive for Business	Site Recycle Bin Second Stage Recycle Bin	93 days 93 days
Notes: (1) Default retention is 30 days. (2) Default retention is 14 days.		

Document Versioning

If the Document Versioning feature is turned on, OneDrive for Business retains a number of previous

versions for each file that has been modified, and end users are then able to restore back to any of these previous versions. However, this does not provide protection against intentional or accidental deletion since all versions of a document are deleted when the current version is deleted.

High Availability and Site Collection Backups

Microsoft uses Database Availability Groups (DAGs) to protect Exchange Online data. While DAGs do a great job of ensuring up-time and preventing catastrophic disasters, they do not protect against mailbox corruption, nor can they restore individual email-related items or entire mailboxes to a point in time. For SharePoint Online and OneDrive for Business, Microsoft takes backups of site collections every 12 hours and keeps these backups for 14 days. IT administrators have no control over these backups or restores. If a restore is necessary, it can only be initiated by contacting Office 365 support. You also cannot restore a single item, document, asset, or library. A full restore of a site collection is the only option.

Mailbox and Account Retention

When an employee leaves an organization, all data in that user's Exchange Online mailbox and OneDrive for Business account is permanently deleted 30 days after their account is deleted. To retain this data for future reference or use, it must be backed up or moved elsewhere. Exchange Online mailboxes can be kept for longer periods of time by configuring an In-Place Hold before the account is deleted; however, this is a premium feature not available in some Office 365 plans.

Microsoft does all they can to put safeguards in place to prevent their customers from losing data, but Microsoft Office 365 does not specialize in data backup and recovery. Seeking an additional layer of protection against accidental or malicious data loss, organizations have begun to use third-party backup solutions that offer enhanced protection of Office 365 data, longer retention periods, and more robust recovery options.

Complete Protection with Barracuda Cloud-to-Cloud Backup

Barracuda Backup is the leading integrated backup appliance in the world according to IDC's Purpose-Built Backup Appliance Tracker. Barracuda Backup was built from the ground up around the cloud with features like built-in cloud replication and management. With a strong legacy in on-premises physical and virtual server protection, Barracuda Backup now includes Cloud-to-Cloud Backup for Office 365. Cloud-to-Cloud Backup protects Exchange Online, SharePoint Online, and OneDrive for Business data by backing it up directly to Barracuda Cloud Storage. Cloud-to-Cloud Backup for Office 365 can be used as an add-on to on-premises Barracuda Backup devices or as a standalone

subscription.

Exchange Online

In backing up Exchange Online, Barracuda Cloud-to-Cloud Backup protects all email messages, attachments, and the complete folder structure of each user mailbox. Messages, folders, or entire mailboxes can be restored back to the original account, a different account, or exported via the download feature.

OneDrive for Business

When backing up OneDrive for Business using Barracuda Cloud-to-Cloud Backup, all files under the Documents Library, including the entire folder structure, are protected. Just like with Exchange Online, files, folders, or entire accounts can be restored back to the original account, a different account, or exported via the download feature.

SharePoint Online

Barracuda Cloud-to-Cloud Backup provides complete protection of SharePoint Online. With item-level recovery options, items can be restored back directly into SharePoint Online from the backups of Document Libraries, Site Page Libraries, and Picture Libraries in Team Site, Publishing Site, and Wiki Site. Barracuda Cloud-to-Cloud Backup for Office 365 eliminates the risk of lost content due to accidental or malicious deletion. You can also retain email messages and files indefinitely if users were to leave your organization—all without having to purchase additional licenses.

Cloud-to-Cloud Backup Features

- **Automated and on-demand backups** – Microsoft Office 365 backups can be fully automated by creating customizable backup schedules to back up data when you want or you can choose to run backups on-demand at any given time. Optionally, backup schedules can be repeated throughout the day as necessary to protect critical data. All Exchange Online, SharePoint Online, and OneDrive for Business data is deduplicated and compressed for maximum storage efficiency and reduced backup windows before being stored in the Barracuda Cloud.
- **Quick and easy restore** – All Office 365 data backed up to the Barracuda Cloud is accessible, searchable, and retrievable from anywhere with an Internet connection. By selecting specific dates from a built-in calendar, point-in-time recovery of data–mailboxes, folders, files, sites, libraries, and email messages–can be achieved. Files or email messages can be restored back to the original user account and location, to a different location within the account, or a completely different user account. Items backed up from SharePoint Online sites can be recovered back to their original location. If you are looking for a specific file or message but are unsure of its location, use the search feature to quickly and easily find the item, as well as where it can be restored or downloaded. Downloading folders puts them into a compressed ZIP file for quick downloads, while email messages are downloaded using the industry-standard EML

format. Files are downloaded using their same file format (unless multiple files are selected), then they are put into a ZIP file for easier access.

- **Reporting and statistics** – For IT Administrators, detailed reporting and audit logging are a key component of a backup solution. Barracuda Cloud-to-Cloud Backup provides backup status and health monitoring for each backup source. Automated email alerts are delivered after each backup to specified email recipients containing a summary of the backup and detailed information about which email messages, folders, and files were added, modified, and removed since the last backup. On the **Status** page, graphs show the number of items added and amount of data backed up each day. Storage statistics and graphs detail how much data has been backed up overall and the storage efficiency, as well as how much data is actually being stored in the Barracuda Cloud after deduplication and compression. An Audit Log tracks and provides details about every action performed within the Cloud-to-Cloud Backup interface.
- **Usability** – Barracuda Backup has always been known for ease of use, and the Cloud-to-Cloud Backup features are no exception. Existing Barracuda Backup users will feel right at home with this new functionality, and new users will be able to learn it within minutes. The Cloud-to-Cloud Backup service is listed among other Barracuda Backup appliances in Barracuda Cloud Control for easy access and management.
- **Administration and policy management** – All Barracuda Backup appliances and Cloud-to-Cloud Backup services can be managed through a single pane of glass with Barracuda Cloud Control—Barracuda's cloud-hosted centralized management interface. Barracuda Cloud Control can be accessed from anywhere with an Internet connection, making it possible to access and recover your organization's data at a moment's notice. By downloading the Barracuda Cloud Control Mobile App, you can view the health status of your backups and backup appliances from your Apple iOS or Android mobile devices. Barracuda Cloud Control also provides role-based administration, allowing you to add and remove users, assign product entitlements, and control access to what functions they can perform in Barracuda Backup and Cloud-to-Cloud Backup. Creating flexible and fully customizable retention policies is easy by allowing you to specify how long to keep your organization's historical data. Create global retention policies for all Office 365 data or get more granular by creating different policies for different users or sets of data. A handy retention calendar visually lays out what your retention timeline will look like on-the-fly.
- **Security** – One of the largest concerns for organization's looking to protect their data in the cloud is security. With Barracuda Backup, all Office 365 data is encrypted in-transit with 128-bit SSL encryption, the same level of security used by most banks and financial institutions. Data stored in the Barracuda Cloud is encrypted at-rest using 256-bit AES encryption. Barracuda Cloud Storage regularly undergoes third-party audits and is SSAE 16 Type II certified. Additional layers of protection included in Barracuda Cloud Control are multifactor authentication, IP address login restrictions, and role-based administration. See the Barracuda website for more information.

With Barracuda Cloud-to-Cloud Backup, you still own your data even though it is in Office 365. Although Microsoft does their best to manage your data effectively, you remain ultimately responsible for the protection of that data, just as you did before you moved to Office 365. Mistakes happen—users accidentally delete or overwrite important data. There are also instances when disgruntled employees or hackers take malicious action in deleting or corrupting data. Therefore, you need to ensure you have an effective backup and recovery solution in place. Barracuda Cloud-to-

Cloud Backup provides complete protection for your entire Office 365 environment.