Your Guide to Creating a Comprehensive Microsoft 365 Disaster Recovery Plan

By: David Nevins, Product Innovation Specialist at CoreView

Disaster recovery (DR) is a set of policies, procedures, and tools aimed at restoring and maintaining business continuity in the event of a natural or man-made disaster.

DR involves planning, preparing, and implementing measures to minimize the impact of such events on the organization's essential functions and services. It plays a crucial role in ensuring the availability, integrity, and security of IT systems and data, minimizing downtime, and preventing data loss.

When it comes to Microsoft 365, disaster recovery refers to the strategies and solutions put in place to protect an organization's Microsoft 365 data and services, such as emails, documents, and applications, in the event of a disaster.

Microsoft 365 has built-in features that help maintain service availability, protect data, and facilitate recovery as needed. However, a number of third-party M365 backup and recovery platforms with advanced features also exist that can help create more comprehensive failsafes for Microsoft 365.

Let's talk about everything you need to know to create a comprehensive disaster recovery plan for Microsoft 365. The guide will help you develop a plan that secures not only your data, but also the configurations and policies responsible for managing Microsoft 365

Why Create a Disaster Recovery Plan for Microsoft 365?

Microsoft 365 may be a highly capable productivity solution, but it's still subject to various threats that could impact an organization's operations. By creating a disaster recovery plan for M365, you can protect your business from the following unexpected scenarios:

- **External Attacks:** Microsoft 365 is a target for cybercriminals who might use ransomware, brute-force attacks, or other malicious techniques to compromise accounts, gain unauthorized access to data, or disrupt services.
- **Human Errors:** Accidental deletion of critical data, misconfiguration of settings, or other mistakes by users or administrators can cause data loss or service interruptions.
- **Insider Threats:** Malicious insiders or disgruntled employees might intentionally delete or tamper with critical data, or misuse their access to disrupt services.
- **Legal Requirements:** Organizations operating in regulated industries must have a disaster recovery plan in place to comply with legal and regulatory requirements. Failure to do that can result in fines, penalties, and worse.

What to Include in Your Microsoft 365 Disaster Recovery Plan?

If you want to build a truly comprehensive disaster recovery plan for Microsoft 365, you will have to take both data and configurations into account. There's a variety of data sets and configuration policies that need backing up across different applications and services, such as Office 365, Azure, Azure AD, Intune, SharePoint, Teams, and Exchange Online. Here's an overview of each:

Office 365:

- OneDrive for Business: User files, folder structure, and sharing permissions
- Outlook: Emails, contacts, calendars, tasks, and notes
- Office Apps: Documents, spreadsheets, presentations, and other files created in Word, Excel, PowerPoint, etc.

Azure:

- Virtual Machines: VM configuration, operating system disks, and data disks
- Managed Disks: Snapshots of managed disks for backup
- Azure SQL Database: Full, differential, and transaction log backups
- Azure Blob Storage: Data stored in containers and blobs
- App Services: Web app configuration, app settings, and custom domains

Azure AD:

- Users: User accounts, attributes, and password hashes
- Groups: Group memberships and attributes
- Roles: Custom and built-in roles
- Applications: Application registrations, service principals, and permissions
- Conditional Access Policies: Policies for securing access to applications and services

Intune:

- Device Configuration Profiles: Policies applied to devices
- App Protection Policies: Policies for protecting corporate data in apps
- Compliance Policies: Policies to ensure device compliance
- Application Deployments: Deployed applications and related settings
- Device Inventory: Device information and status

SharePoint:

- Sites: Site collections, subsites, and site templates
- Lists and Libraries: Content and structure of lists and libraries, including metadata
- Permissions: User and group permissions, and site-level security settings
- Customizations: Custom site designs, themes, and web parts

Teams:

- Teams: Team names, descriptions, channels, and settings
- Conversations: Chat history and messages in channels
- Files: Files shared in conversations and stored in the associated SharePoint document library
- Tabs and Apps: Custom tabs and third-party apps integrated with Teams

Exchange Online:

- Mailboxes: User and shared mailboxes, including mailbox folder structure, emails, attachments, and calendar events
- Contacts: User and shared contacts
- Distribution Groups: Distribution group memberships and settings
- Retention Policies: Policies for archiving and deleting messages

Built-in Mechanisms for Disaster Recovery in Microsoft 365

Microsoft 365 includes built-in backup and retention mechanisms up to a certain extent to help organizations protect their data and ensure business continuity. These features are designed to prevent data loss, recover deleted items, and comply with minimum regulatory requirements. However, they also come with several limitations that prevent them from serving as a full-fledged backup and recovery solution. For example:

- **Data Replication:** Microsoft 365 uses data replication across multiple geographically distributed data centers, which helps protect against hardware failures, power outages, and other site-level issues. However, this is not a true backup solution, as it does not allow for point-in-time recovery of data in case of accidental deletions or data corruption.

- **Retention Policies:** Organizations can configure retention policies to preserve data in Exchange Online, SharePoint Online, OneDrive for Business, and Teams for a specified period. However, these policies only cover certain types of data, and configuring them can be complex.

- **Litigation Hold and In-Place Hold:** These features allow organizations to preserve mailbox content and documents in SharePoint and OneDrive for legal or compliance purposes. However, they are not designed to serve as a comprehensive backup solution and may not cover all data types.

- **Versioning:** SharePoint Online and OneDrive for Business support versioning, which allows users to access previous versions of documents. However, versioning only applies to specific file types and may not protect against all types of data loss.

- **Recycle Bin:** Deleted items in SharePoint Online, OneDrive for Business, and Exchange Online are temporarily stored in a recycle bin, allowing for recovery within a specific time frame. However, this is not a long-term backup solution, and once the data is permanently deleted, it cannot be recovered.

Using Third-Party Tools to Implement Better Disaster Recovery

Where built-in backup and retention systems prove insufficient, a number of third-party solutions exist to help you create a more thorough disaster recovery program for Microsoft 365. These tools take advantage of Microsoft's built-in Application Programming Interface (API) to integrate with services like Office 365, Azure, Azure AD, Intune, etc. and pull your data and configurations for storage off-site. Here's a brief overview of how it works:

- **API Authentication:** Third-party tools must first authenticate with Microsoft Graph using OAuth 2.0, which enables secure access to the required data and services. This typically involves registering an application in the Azure Active Directory, obtaining the necessary permissions (scopes), and acquiring access tokens.

- **Accessing Data:** Once authenticated, the third-party tool can make API calls to Microsoft Graph to access data and configurations from various Microsoft 365 services. The API provides granular access to resources like mail, calendar, contacts, files, and more.

- **Incremental Backups:** The Microsoft Graph API supports delta queries, which allow third-party tools to efficiently track changes and only fetch data that has been added, updated, or deleted since the last backup. This enables incremental backups and reduces the amount of data transferred during each backup operation.

- **Storage and Recovery:** The backed-up data can be stored by the third-party solution in a secure and compliant manner, often using encryption and redundancy to ensure data integrity and availability. In the event of data loss or corruption, these tools can use the Microsoft Graph API to restore the data back to Microsoft 365 services.

- **Monitoring and Reporting:** Third-party tools can use the Microsoft Graph API to monitor the backup status, generate reports, and provide alerts for administrators to take appropriate action.

The Best Third-Party Disaster Recovery Solutions for Microsoft 365

If you're looking for a third-party platform to automate your disaster recovery plan for Microsoft 365, there are lots of options to choose from. These tools integrate with Graph API to pull your data from services like Office 365, Azure, Azure AD, and Intune — then storing it securely in an on-premises or cloud-based storage solution. They also offer a number of additional features, such as eDiscovery, to make it easier to back up and selectively recover data sets. For example:

Veeam Backup

Veeam Backup for Microsoft Office 365 is a popular solution designed to protect your organization's data within the Microsoft 365 environment. It ensures that all critical data across Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams is securely backed up — while allowing for on-demand restoration of individual items, such as emails, documents, list items, mailboxes, and folders.

Veeam's solution helps organizations meet compliance requirements by allowing them to maintain control over their Microsoft 365 data. It also provides additional features like eDiscovery to aid in the identification and retrieval of specific data sets. The storage architecture is designed to support organizations of any size, making it a suitable option for small businesses, enterprises, and everything in between.

AvePoint Cloud

AvePoint Cloud Backup is a robust backup and recovery solution for Microsoft 365 that supports Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, Project Online, and more. It performs automatic backups of your data up to four times a day, ensuring that your organization's data remains protected and up-to-date. Organizations can customize their backup schedules to meet their specific requirements and preferences.

AvePoint AvePoint offers unlimited storage for your backups, while also allowing for easy and precise recovery of individual items or entire datasets, depending on your organization's specific needs. Backups are encrypted and stored securely in AvePoint's cloud, which is compliant with various security standards, such as GDPR, HIPAA, and FedRAMP.

Simeon Cloud

Simeon Cloud is an end-to-end solution that automates configuration management for Microsoft 365. Unlike the other platforms on this list, Simeon does not focus on data backup. Instead, it's one of the only tools that specialize in helping you back up and restore your configurations, policies, and settings across Microsoft 365.

Simeon provides automated backup and restore services for a range of Microsoft 365 configurations, including Office 365, Azure, Azure AD, Intune, SharePoint, Teams, and Exchange Online. It allows for granular recovery of specific configurations or entire system states with the click of a button, with full version control and audit logging capabilities.

Want to learn more about how you can use Simeon Cloud to create a backup strategy for your Microsoft 365 configurations as part of your larger disaster recovery plan?

Request a free demo today to find out!

Create a Comprehensive Disaster Recovery Plan by Backing Up Both Your Microsoft 365 Data and Configurations

It's not enough just to back up your files and data. If you want to create a foolproof disaster recovery plan for Microsoft 365, you also have to take the settings, policies, and configurations that power your cloud environment into account.

Microsoft 365 features thousands of potential configurations spread across hundreds of different screens, portals, and dashboards — making it impossible to keep a manual record of your system configurations. So, when your tenant is compromised due to an external attack or internal error, having a backup of those configuration files along with your business data is crucial to ensuring continuity of your cloud infrastructure.

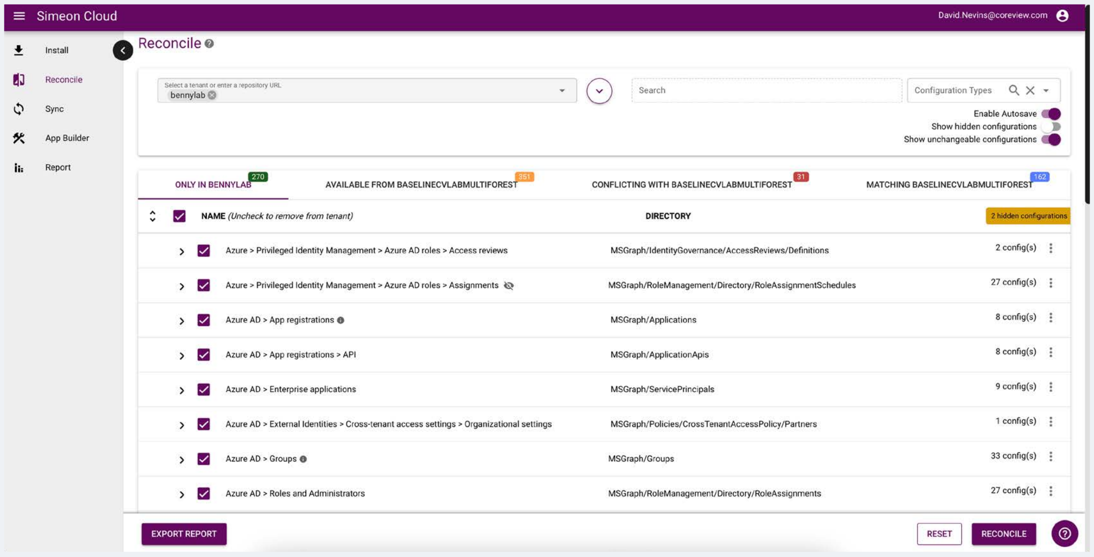
When creating a disaster recovery plan for Microsoft 365, be sure to use both built-in and third-party solutions to create a backup plan for your documents, folders, assets, settings, policies, and configurations. That way, getting up and running after an attack or outage is as easy as falling back to a previous version of your system state.

Simeon Cloud: The Ultimate Disaster Recovery Tool for Microsoft 365 Configurations and Policies

While there's an unending list of data backup solutions to choose for when it comes to Microsoft 365, solutions that enable you to back up your configurations and settings are few and far between. Until recently, your only option would have been to go through the tiresome process of manually create PowerShell scripts to pull your configurations using Microsoft Graph so that you can store them in an offsite location.

However, Simeon Cloud is the first premium automation tool that enables you to back up your configuration files using a no-code web interface. The process is faster, more efficient, and more resilient against the changing compliance landscape.

Want to learn more about how you can use Simeon Cloud to create a backup strategy for your M365 configurations as part of your larger disaster recovery plan? [Request a free demo today to find out]!



Reconcile

Select a tenant or enter a repository URL: bennylab

Search

Configuration Types

Enable Autosave ●
Show hidden configurations ○
Show unchangeable configurations ●

ONLY IN BENNYLAB 270 | AVAILABLE FROM BASELINECVLABMULTIFOREST 351 | CONFLICTING WITH BASELINECVLABMULTIFOREST 31 | MATCHING BASELINECVLABMULTIFOREST 162

☑	NAME *(Uncheck to remove from tenant)*	DIRECTORY	2 hidden configurations
☑	Azure > Privileged Identity Management > Azure AD roles > Access reviews	MSGraph/IdentityGovernance/AccessReviews/Definitions	2 config(s)
☑	Azure > Privileged Identity Management > Azure AD roles > Assignments	MSGraph/RoleManagement/Directory/RoleAssignmentSchedules	27 config(s)
☑	Azure AD > App registrations	MSGraph/Applications	8 config(s)
☑	Azure AD > App registrations > API	MSGraph/ApplicationApis	8 config(s)
☑	Azure AD > Enterprise applications	MSGraph/ServicePrincipals	9 config(s)
☑	Azure AD > External Identities > Cross-tenant access settings > Organizational settings	MSGraph/Policies/CrossTenantAccessPolicy/Partners	1 config(s)
☑	Azure AD > Groups	MSGraph/Groups	33 config(s)
☑	Azure AD > Roles and Administrators	MSGraph/RoleManagement/Directory/RoleAssignments	27 config(s)

CoreView