NAKIVO

White Paper

White paper: Microsoft Office 365 and Data Protection

Risks in Shared Responsibility

Executive Summary

Millions of businesses rely on Microsoft Office 365. Users of this productivity suite think their data is safely stored in the cloud and that Microsoft offers backup and recovery features. This is a dangerous misconception. Microsoft's "shared responsibility model" specifies that Microsoft is responsible for infrastructure maintenance while users are responsible for the bulk of data protection. As a result, businesses must clearly understand their share of responsibilities when using Microsoft Office 365 and the threats they face if they fail to protect their data.

Section 1: Data Management and Data Responsibilities

Defines the key concepts guiding businesses' management of Microsoft Office 365 data: availability, accessibility and security. Section 1 then introduces how Microsoft divides the data cycle into separate responsibilities between a business and Microsoft.

Section 2: The Shared Responsibility Model

Explains how data responsibility is shared between Microsoft and users of Microsoft Office 365. Microsoft is responsible for the physical and virtual infrastructure (physical protection, data replication, system maintenance and user/administrative control architecture). The Microsoft Office 365 user is responsible for data protection (data classification, data backup and data recovery).

Section 3: The Four Threats to Microsoft Office 365 Data

Identifies businesses' risk exposures if they fail to protect their Microsoft Office 365 data. The threats are accidental deletion, security vulnerabilities, legal and compliance penalties and retention policy gaps.

Section 4: Countering Threats with Third-Party Solutions

Explains how solutions like NAKIVO Backup & Replication can mitigate the risks businesses face when using Microsoft Office 365.

Section 5: NAKIVO Backup & Replication

Offers an overview of how the software solution protects virtual, physical, cloud and SaaS environments.

1. Data Management and Data Responsibility

Businesses using Microsoft Office 365 must ensure that their data is available, accessible and secure. Businesses pursue these goals to boost operational efficiency while also protecting against threats and compliance issues.

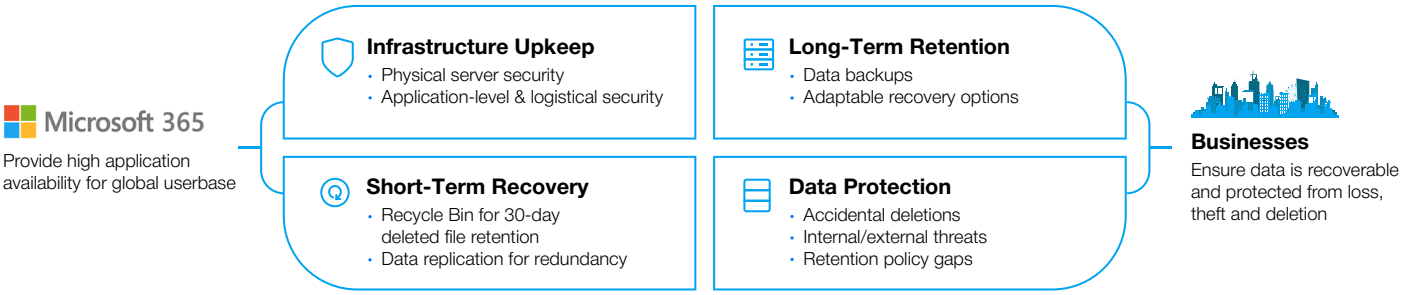
- Availability refers to users being able to run applications and use data without interruptions.
- Accessibility refers to users being able to retrieve necessary data across short, medium and long timeframes.
- Security refers to protecting data from theft, corruption, deletion or access by unauthorized users.

Businesses using software that is installed on their servers are fully responsible for data accessibility, availability and security. Microsoft, however, offers Microsoft Office 365 as a software as a service (SaaS), that is, businesses pay for a service hosted in the cloud. This means that the data life cycle is divided between Microsoft and the business. Microsoft clearly defines this division of responsibilities in their Software Licensing Agreement. In this discussion, data responsibility takes two forms: firstly, legal and regulatory requirements that businesses must comply with and, secondly, steps businesses should take to employ best data protection practices.

2. The Shared Responsibility Model: Microsoft vs. Microsoft Office 365 User

Microsoft uses the “shared responsibility” model to divide the data life cycle between Microsoft and the Microsoft Office 365 user. Microsoft is responsible for maintaining the infrastructure that allows Microsoft Office 365 to run smoothly and reliably. Users, on the other hand, are responsible for protecting their Microsoft Office 365 data. This means that Microsoft is not responsible for restoring lost, stolen, or deleted data outside of limited retention policies.

Microsoft Office 365 retains deleted data for 30 days in the recycle bin and deleted groups and mailboxes for 14 days. These policies are designed to correct user and administrative errors in the short-term. Microsoft Office 365 also includes the Litigation Hold for Enterprise users. This feature prevents data from being deleted for regulatory compliance. It is the user’s responsibility to employ a long-term data storage, backup and recovery solution to protect Microsoft Office 365 data.



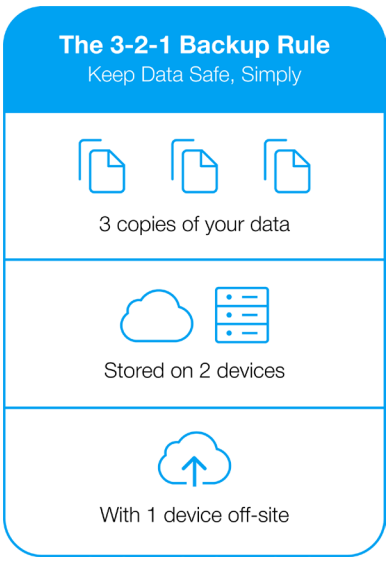
2.1 Microsoft's "shared responsibility": application up-time and a strong infrastructure

Microsoft's focus is to make sure that Microsoft Office 365 is available and operates smoothly for its global userbase. As a result, Microsoft is responsible for the physical and virtual infrastructure necessary for using Microsoft Office 365. Microsoft fulfills its share of responsibility by providing:

- **Physical protection** of the hosting servers from natural disasters and criminal acts.
- **Data replication** for the purpose of redundancy. If files become corrupted, the data will instantly fail over to replicated versions without disruptions for the user. This may keep data accessible in the short term, but it is not a substitute for data backups. Backups provide recoverability for situations in which Microsoft Office 365 objects are deleted but are later needed in the future. Replication does not serve this use case because if an object is deleted, the deletion is replicated across every copy.
- **System maintenance** so that the cloud-based applications are available, smooth and reliable for the global userbase. This includes network and application-level controls for Microsoft Office 365.
- **User/administrative control architecture** to ensure access is only granted to users with the proper credentials. Microsoft is not responsible if a bad actor steals the proper credentials and accesses data without authorization. Microsoft builds and repairs the gate and keys, but the users have to keep the keys safe.

2.2 Microsoft Office 365 users' "shared responsibility": data protection

Microsoft Office 365 users can rely on Microsoft to provide an industry-leading productivity suite, but they must count on themselves for medium- and long-term data recoverability. Broadly, the objectives of data protection are data availability, accessibility and preservation. For a Microsoft Office 365 user to protect data effectively, they should employ three processes: data classification, data backup and data recovery. Microsoft does not offer these processes under the shared responsibility model. Instead, it is the user's job to understand what the processes are and how they work together.



Data classification is the process through which a business identifies, maps and tags its data according to important categories. The primary purpose of classification is to make sure that only authorized persons can access business-sensitive data. More broadly, however, data classification transforms a business's messy pool of dispersed data into a navigable roadmap. This, in turn, provides the foundation for an accurate and effective data management system. Specifically, it ensures all data is properly accounted for during backup and recovery planning. It also simplifies e-discovery searches if a business needs to track data for compliance reasons or to fulfill legal requests.

Data backup is the core of a Microsoft Office 365 user's responsibility in the "shared responsibility model". The purpose of data backup is to ensure that if a disaster occurs, a business's data is safe. The central guideline is the 3-2-1 backup rule — make sure there are at least three copies of data, stored on two storage devices, with one of them stored off-premises. For a Microsoft Office 365 user, this means using a combination of on-site physical backups and third-party cloud backup solutions to guarantee data resilience. There is a wide range of backup methods that vary in granularity, recovery speed, storage size, and affordability. More information on the specific methods can be found here.

Data recovery is the process by which a user restores data from a backup. The type of backup determines the speed and granularity of the recovery. Recoveries can range from near-instant single file restoration to a business's Microsoft Office 365 entire data library.

3. The Four Threats to Microsoft Office 365 Data

Many businesses incorrectly believe that Microsoft's responsibilities include data protection. Operating under this dangerous misconception exposes a business to four threats:

- accidental deletions
- external and internal security vulnerabilities
- legal and compliance penalties
- retention policy gaps

These threats can incur serious financial costs, reputational damage and operational disruptions. A business can limit the chance and impact of these risks by fulfilling their portion of the "shared responsibility model." This requires a business to implement a data protection strategy that covers data classification, data backup and data recovery.

3.1 Accidental deletion

An accidental deletion is an unintentional deletion by an authorized user. This threat, while simple and avoidable, is common and capable of significant damage. Microsoft Office 365 offers some built-in features to address this threat, such as the Recycle Bin and Recoverable Items folder. If a user deletes an email, for example, the email will go to the Recoverable Items

folder for up to 30 days, depending on the retention policy. This is called a soft deletion. After 30 days or less, the email is permanently deleted. This is a hard deletion.

The native retention policy tools in Microsoft Office 365 are short-term oriented and require the user to recognize the mistake within the retention policy timeline. They are intended for cases involving a user putting the wrong folder in the Recycle Bin or accidently deleting an email. These Microsoft Office 365 features offer no redundancy if an administrator permanently deletes an inbox during routine maintenance or if an accidental deletion goes unnoticed. In short, these features are intended to fix individual-level mistakes during the normal workflow. They are not intended for nor capable of recovering entire mailboxes or accounts if an error happens at the administrator-level.

Businesses can virtually eliminate the impact of accidental deletions by following the best backup and recovery practices. Employing best practices can ensure that deleted data is easily and quickly recoverable.

3.2 Security vulnerabilities: internal and external

In the modern business environment, competitors, black hat hackers and disgruntled employees regularly target businesses' data for financial and personal reasons. Cybersecurity practitioners divide these vulnerabilities into external and internal threats. Threats that emerge from actors outside of the business, such as competitors and black hat hackers, are external. Threats that emerge from actors inside the business, such as disgruntled current and former employees, are internal. Specifically, in terms of Microsoft Office 365, these actors will delete data to disrupt operations or use ransomware to force businesses into paying large sums of money to regain access to the data. Microsoft offers no substantive protection beyond the software's native security architecture.

3.2.1 Internal threats

Unhappy current and former employees may sabotage a business's operations by intentionally deleting files from Microsoft Office 365. If they have the necessary access, they could permanently purge data from servers. The first line of defense is staff oversight techniques and tight user controls. Staff oversight requires a system to monitor employee satisfaction and identify potential problems before they occur. Tight user controls require using data classification to ensure that employees only have access to data relevant to their position. If an employee nevertheless deletes data, a business should have backups on hand to quickly recover the lost data, thereby ensuring business continuity.

3.2.2 External threats

Competitors and black hat hackers will use computer network attacks (CNAs) and social engineering to target a business's data. CNAs exploit vulnerabilities in software to gain access to applications and deploy malicious malware. Social engineering is a method by which

attackers manipulate users into willingly helping the attacker gain access to a network. Once in the network, the attacker can access data and easily deploy malware.

Microsoft is responsible for providing the baseline security architecture to protect users from CNAs. It's a game of cat-and-mouse, however, and security patches are often one step behind. Furthermore, social engineering allows attackers to bypass security protections by gaining access directly from an employee. Safeguarded backups significantly diminish the impact of these attacks. This, in turn, ensures that businesses do not have to pay ransomware attackers or permanently lose business-critical information.

3.3 Legal and compliance penalties

Businesses must maintain data archives to meet financial regulations, produce evidence for legal cases and document consumer data use. For businesses with operations or clients in the USA, for example, the Sarbanes-Oxley Act of 2002 requires businesses to store financial data for reporting. The Federal Rules of Civil Procedure forces businesses to preserve and submit data relevant to court cases. Consumer data laws, such as the General Data Protection Regulation (GDPR) in the European Union, stipulates that businesses must document how they use consumer data and provide evidence of its deletion upon request.

Microsoft Office 365 offers limited functionality to help businesses observe legal and regulatory requirements. The Litigation Hold feature will permanently freeze data, preventing deletion, but storage is limited to 100 GB. Large businesses will exceed this limit. Furthermore, Litigation Holds only work with currently available data, which means that previously purged data is inaccessible. If a business is not able to recover data for legal or regulatory requirements, it is the user's responsibility, not Microsoft's. Businesses need to look to third-party backup and recovery solutions to stay on the right side of the law.

3.4 Retention policy gaps

Data management describes how a business organizes the use, storage and protection of data. If a data management strategy fails to completely address how data is retained, policy gaps emerge. These gaps—or protection failures—expose the business to operational and legal risks. This section focuses on the operational disruptions. Retention policy gaps in Microsoft Office 365 are often formed by:

- neglecting to back up former employee data
- inadequate backup rules
- data loss during migrations

3.4.1 Neglecting to back up former employee data

Businesses commonly deactivate an employee's account if the employee leaves the company. Microsoft will automatically delete an inactive user account and all of the account's associated data after 90 days. Furthermore, with the employee gone, it's common for businesses to lose track of important data assigned to that employee's user account. If that important data is not backed up, the business will not be able to recover it after the retention period ends.

3.4.2 Inadequate backup rules

An effective backup policy requires a business to choose appropriate recovery time objectives (RTO) and recovery point objectives (RPO). An RTO is how much time a business can spend recovering from a disaster. An RPO is how much information a business can afford to lose if a disaster occurs. More detailed information on these metrics can be found here.

Microsoft Office 365 does not offer a native backup function, which means that businesses must incorporate third-party backup and recovery solutions into their Microsoft Office 365 operations. While these solutions will provide the technical capabilities, businesses must still define their RPOs and RTOs as part of the data management process.

3.4.3 Data loss during migrations and transitions

Businesses can deploy Microsoft Office 365 in on-premise, cloud and hybrid environments. Each environment offers different benefits for different businesses. The risk of data loss emerges during migrations from on-premise to hybrid/cloud environments or hybrid to cloud environments. When a business is accustomed to a certain Microsoft Office 365 environment, it will likely have established backup processes. During migration, however, these processes will become disrupted. This raises the chance that retention policy gaps could emerge, resulting in data loss.

4. Countering Threats with Third-Party Solutions

Businesses can fulfill their portion of the shared responsibility model by combining Microsoft Office 365 with third-party backup and recovery solutions. Options on the market, such as NAKIVO Backup & Replication, empower businesses to protect themselves from the major threats facing Microsoft Office 365 data.

Accidental Deletion: Backups significantly limit the damage from accidental deletions by creating readily recoverable copies of the lost data. NAKIVO Backup & Replication enables granular recoveries for Exchange Online, allowing users to restore individual mailboxes, mailbox folders and emails directly from backups.

Threats to Microsoft Office 365 Data

Accidental Deletion

Costly yet preventable, accidental deletion is the leading cause of data loss among businesses.

Retention Policy Gaps

Employee turnover, data migrations and changing circumstances create unforeseen holes in your data protection.

Security Vulnerabilities

Insider threats, ransomware hackers and competitors all see your data as a lucrative target.

Legal & Compliance Penalties

Whether for financinal reporting or court cases, if you've lost the data then you're liable.

Security Vulnerabilities: Third-party backup and recovery solutions enable businesses to recover data lost through a cyber-attack deletion or ransomware attack. The ability to restore ransomed data allows businesses to avoid paying to regain access. Businesses must look to third-party cybersecurity platforms, however, to raise the overall security of their environment.

Legal and Compliance Penalties: Businesses can avoid financial and reputational costs by backing up important data for reporting and litigation requirements. NAKIVO Backup & Replication includes object level recovery, allowing users to quickly search and restore Exchange Online items from backups without running a full recovery.

Retention Policy Gaps: NAKIVO Backup & Replication provides businesses with a unified solution to schedule backups, designate backup destinations, set retention policies and run recoveries. This ensures that they can put former employees' Exchange Online data in secure long-term storage, set appropriate backup rules and consolidate data in backups for migrations.

Comprehensive Data Protection with NAKIVO Backup & Replication

NAKIVO Backup & Replication is a fast, reliable and affordable solution that delivers backup, replication, instant granular recovery and disaster recovery in a single pane of glass. The product protects virtual, physical, cloud and SaaS environments. NAKIVO Backup & Replication offers advanced features that increase backup performance, improve reliability and speed up recovery.

Deploy in under 1 minute
Pre-configured VMware VA, Nutanix AHV and AWS AMI; 1-click deployment on ASUSTOR, QNAP, Synology, NETGEAR, FreeNAS and WD NAS; 1-click Windows installer, 1-command Linux installer.

Protect Data Across Platforms
Native, agentless, image-based, application-aware backup for VMware, Hyper-V, AWS EC2, Nutanix AHV; Windows/Linux physical servers and Windows workstations; Microsoft Office 365 application data; Oracle databases.

Streamline data protection
Automatically protect machines matching policy rules, which can be based on machine name, tag, size, location, and so on.

Increase backup speed
Global backup deduplication, adjustable backup compression.

Reduce backup size
Incremental backups with CBT/RCT/CRT, LAN-free data transfer, network acceleration; up to 2X performance when installed on NAS

Decrease recovery time
Instant recovery of VMs, files, and application objects (Exchange, Active Directory and SQL); automated Site Recovery; near-instant P2V recovery.

Ensure recoverability
Instant backup verification with screenshots of test-recovered VMs; backup copies offsite, to tape or AWS/Azure clouds.

Simplify management
Simple, fast, easy-to-use web interface, accessible anytime and anywhere – even from a mobile device.

About NAKIVO

NAKIVO is a US-based corporation dedicated to delivering the ultimate backup and site recovery solution. With 20 consecutive quarters of double-digit growth, 5-star online community reviews, 98% customer satisfaction with support, and more than 14,000 paid customers worldwide, NAKIVO provides an unprecedented level of protection for virtual, physical, cloud and SaaS environments. As one of the fastest-growing data protection software vendors in the industry, NAKIVO provides a data protection solution for major companies such as Coca-Cola, Honda, and China Airlines, in addition to working with over 4,100 channel partners in 140 countries worldwide. Learn more at www.nakivo.com.