



Doc. No. RMD-I-2021-02

Effective Date: 03/26/2021

Version: 1.0

Microsoft 365 Handbook

Microsoft 365 is an all-in-one solution that allows colleagues to collaborate, utilize secure document storage, and manage operating systems. MS 365 allows employees to fulfill records management responsibilities without moving information out of MS 365.

Why MS 365?

Flexibility and mobility

- Employees can open, view, and edit documents from supported web browsers on desktop computer or mobile devices.

Share and Collaborate

- Employees can collaborate and easily share and co-edit documents, saving time and confusion that comes from emailing documents back and forth.
- Employees can communicate using a group chat platform that puts all team conversations, files, meetings, and apps in a single, shared, easily-accessible workspace.
- Employees can make video calls, hold web conferences, send instant messages, make voice calls and keep track of ideas and meeting notes.

Manage Updates and Devices

- The MS 365 application is always up-to-date.
- A simplified setup means the management of employee devices and services is done using one administrative set up.

Stay Secure

- IT employees can protect sensitive information across devices with always-on security.
- Simplify the setup and management of employee devices and services with a single I.T. console.
- Built-in spam and malware protection for email means information will be better protected in the cloud.

What applications are available in MS 365?

Office Apps — Word, Excel, PowerPoint, OneNote, Access, Office Online

Email and Calendar Outlook — Exchange Online

File Storage—OneDrive for Business

Business Intelligence—Power BI

Social, Video, Sites —Teams, Yammer, SharePoint Online, Planner

Threat Protection—Microsoft Advanced Threat Analytics, Device Guard, Credential Guard, AppLocker, Windows Information Protection

Identity and Access Management —Azure Active Directory — SSPR Cloud Identities, MFA, SSO

Information Protection—Litigation Hold, eDiscovery, Compliance Manager, Data Subject Requests, Windows Defender Antivirus, and BitLocker encryption sensitive information covered under HIPAA.



Who uses MS 365? How can you manage information in MS 365?

There are two roles in MS 365: **Creators** and **Custodians**

Creators:

You! You create information every day. When the information that you create qualifies as a record, it is required to be retained for a certain amount of time for legal, operational and historical reasons. When you save information onto SharePoint (or any non-One Drive MS 365 system), you are doing your part as a creator. An appointed expert --a **custodian**-- will help label information with rules for retention, discovery, and disposition. Why is One Drive different? Answer below!

Custodians

A custodian is an expert who is trained in understanding record keeping requirements and the technology we use to identify information and all subsequent rules and requirements. That person may be a Records Management Officer (RMO) that person may work for Agency IT or that person may work at DOITT. That person would partner with DORIS and Agency management, legal and IT to label information created in libraries that will dictate retention, identification, and disposition.

How is MS 365 different from old methods of Record Retention?

To identify and locate records, records programs have traditionally created storage spaces (both physical and digital) and moved records to those spaces (such as physical warehouse or shared drives). MS 365 retains information like a relational database. The information stays in one place but RMOs/custodians can assign attributes (called labels in MS 365) to information and that information will retain that label for its lifecycle. Labels can be used for search and other identification workflows and will be discussed in more detail below.

What are the important questions for Records Management in MS 365?

What are Records?

All documents, data, and information made or received pursuant to law or ordinance, or in connection with the transaction of official city business are municipal records.¹ By using retention labels, you can implement a single and consistent strategy for managing information across your Microsoft 365 environment. When labeled information reaches its required retention period, that information should be disposed through the disposition approval process.

What is an Information Lifecycle?

Information must be retained for business use and for legal and regulatory reasons and for long-term historical preservation. For every kind of record, both DORIS and your local RMO/custodian have done extensive research to determine the appropriate retention period. When those retention periods expire, the records should be securely disposed. The proper retention periods and methods of disposal are detailed in the [NYC Supplemental Record Retention Schedule](#).

Where do I retain information in MS 365 (OneDrive vs. SharePoint)?

OneDrive and SharePoint are both retention repositories for file storage,. SharePoint includes many additional features such as collaboration tools and dashboards while OneDrive is typically used by individuals and business teams who need a central location to store and access and edit files. OneDrive is more than an online filing cabinet but allows for versioning and sharing to make it easy to work together.

¹ See N.Y.C. Charter Chap. 72, § 3011(2). For further information, see "[Definition of a Record Under the NYC Charter](#)".



SharePoint is a collaboration tool for businesses that need multiple individuals and teams to work on documents and products simultaneously.

While you are working on a file by yourself, save it to OneDrive. Your OneDrive files are private unless you share them with others, which is particularly useful if you have not created an appropriate team yet.

When documents that you start by yourself grow in importance and require collaboration from multiple users, move these documents from OneDrive to SharePoint. When you need a new shared location to store team files, create a shared library right from OneDrive, add members, and start working together. These libraries are accessible within Teams, SharePoint, and Outlook. It is easy to copy or move files where you and others need them.

Best practices in MS 365

Define roles at your agency and leverage expertise outside your agency

Most of the Records Management process will be owned by Custodians, with support from DORIS, DOITT and Agency IT.

- DORIS will own the guidance documentation (policies, schedules) and label plans; train custodians and IT employees; perform compliance audits and answer any questions from all city employees.
- IT (both agency and DOITT) teams will implement systems that efficiently support your records management process.
- RMOs/custodians will manage the labeling of information at agencies.
- End-users may also label information and must understand the day-to-day processes.

Organize and Govern

Each agency RMO/custodian is the default ‘owner’ of information for their agency. Permission-based roles should be established. It is important for custodians to inspect informational usage in the organization to determine how and which documents and other content types are labeled. This labelling should be defined first before adopting SharePoint as your System of Record.

DORIS will establish requirements in city-wide policies and schedules, which agencies must meet, as well as labels. All information must contain labels that detail when that information is no longer active, how long it should be retained after it is no longer active plus how it should be disposed.

Create Sites

Retaining information for business use requires planning and organization. MS 365 allows users to save information together in a grouping called a “site”. Often sites are grouped together if they perform a similar function or are created and maintained by one group of employees. To create a site, your Agency IT support staff must create a ticket in Remedy and DOITT will create that site, meeting your agency’s specifications.

Use Labels

To make searching for information easier, it makes sense to apply labels to information. Labels are short descriptions or tags ascribed to files that allows information managers to classify information across the various MS 365 platforms. For example, a user may apply a label called ‘Contracts’ to a document, which will ensure that the record is retained until the retention period has expired (e.g., 7 years) and will also easily be found in a search for “contracts”.

Custodians can define the labels and policies, then publish the labels for use. Creators or Custodians can then use the labels to classify documents.

MS 365 automatically enforces retention rules and can even automatically attribute label-based criteria set by the RMO/custodian (This is particularly helpful with things like sensitive information). Ultimately, labels give information managers the ability to universally set information management policies and use



MS 365 to enforce those policies across a wide array of systems and applications across the MS 365 environments.

As retention, search, disposition, and eDiscovery are driven by good information architecture, please use only DORIS-approved labels.

These are things labels can help with:

1. You can label information as a record. Create and configure retention labels to mark content as a record that users can then apply or automatically apply by identifying sensitive information, keywords, or content types.
2. Migrate from network drives and manage your retention requirements with a file plan. By using a file plan, you can import an existing retention plan to Microsoft 365 or build a new one for enhanced management capabilities.
3. Configure retention and deletion settings with retention labels. Configure retention labels with the retention periods and actions based on various factors that include the date last modified or created.
4. Start different retention periods when an event occurs with event-based retention.
5. Review and validate disposition with disposition reviews and proof of information deletion.
6. Export information about all disposed items with the export option.
7. Set specific permissions for records manager functions in your organization to have the right access.

Additional Functionalities in MS 365

Reporting and auditing

MS 365 provides several tools allowing creators and custodians to monitor the life r information to ensure they comply with your internal policies. Custodians should review sites/information to ensure that they have been properly labeled. A DORIS auditor should receive annual attestations of completed labeling from custodians.

eDiscovery/Legal Holds

If information may be used in a litigation, custodians can place information on hold in multiple ways for eDiscovery (using either the either Core eDiscovery or Advanced eDiscovery apps). If content is subject to both retention settings and an eDiscovery hold, preserving content for the eDiscovery hold always takes precedence.

Sensitivity/Privacy

Information can also be labeled to indicate sensitivity or privacy. Personally Identifiable Information can be anonymized or encrypted or viewed only by a small and well-maintained access list.

Reviews and approvals at the end of its retention period

Information that has met its business (active and semi-active information) and legal (fiscal, legal holds, etc.) retention requirements are triggered for disposition by an agency records manager. The disposition process does not include information labeled for Auto Deletion, per the [Automatic Deletion of Data Policy](#).

The disposal process includes multi-agency reviews:

- Agency Counsel (review for legal holds, privileged information, timeliness)
- NYC Law Department (review for legal holds, privileged information, time, etc.)
- DORIS
 - Records Management: Series, extents, and dates are accurate and in line with disposition schedule;



- Municipal Archives: Review for historical records, sampling opportunities, record formats, PII, privileged information and general information gathering;
- DORIS Commissioner: Review for records management, archival, and library content...need better language
- Once each agency and appropriate divisions conduct the review, the information is either destroyed, or formally transferred to the Municipal Archives. The agency transfers legal ownership of the materials to the Municipal Archive The Archives processes, preserves and manages access to the collections as required by the City Charter.

As mentioned above, any information on legal hold cannot be disposed of even if its retention period is over. Consult with the agency Legal Department if you believe a legal hold is no longer in effect and eligible information should be disposed.

Proof of disposition for content that is permanently deleted at the end of its retention period.

All information disposed in MS 365 is detailed in a certification/disposition report that is sent to both custodians and approvers. When transferred to the Archives, the documentation is assigned an accession number.