OneDrive for Business: Best Practices and Usage

September 2020
Version 2.0

Contents

Purpose

Many state and local governments have moved to hosted solutions for both hardware and software. It reduces the need for large investments in hardware/software and storage and allows employees to access documents and tools from offsite locations or from multiple devices. As government moves to become more efficient and its employees work from multiple locations, its employees need a tool to allow them to collaborate and manage versions of documents and work product. Information is stored remotely on servers owned by Microsoft and located in the continental United States. This concept of storing information in a remote location is often referred to as cloud storage. For more information on records management and cloud storage for North Carolina state agencies, please see *Cloud Computing and Public Records,* available at **https://archives.ncdcr.gov/documents/best-practices-cloud-computing-records-management-considerations**.

The Department of Information Technology (DIT) has purchased Microsoft Office365 for state agencies, including access to Microsoft SharePoint and OneDrive for Business. Office365 includes the latest version of Microsoft Office software (Word, Excel, PowerPoint) in the OneDrive for Business package so users can make changes to documents from different devices, even if they do not have the software locally installed. OneDrive for Business is similar to other cloud storage and sync options such as Dropbox, iCloud, and Google Drive. However, OneDrive for Business is an approved tool for use with state information and provides employees the ability to access from multiple devices. Unlike Dropbox, iCloud, and Google Drive, OneDrive for Business access is authenticated and authorized by the employee's NCID account; therefore, any document stored there will become inaccessible after an employee separates from the agency. OneDrive for Business can store multiple file formats including images and video, as well as Microsoft Office formats. OneDrive for Business is compatible across multiple operating platforms and browsers, including Apple iOS, Android, and Linux. Of major concern, however, is that once an employee leaves an agency or terminates employment with the state, information stored on their OneDrive for Business will become inaccessible and unrecoverable, since the account will be closed.

These guidelines offer guidance and best practices in the following areas:

- Definitions of SharePoint and OneDrive for Business
- Purpose of SharePoint and OneDrive for Business
- Use of SharePoint and OneDrive for Business and related tools by public service employees
- An overview of O365 tools that store information in SharePoint and OneDrive
- Maintaining continued accessibility of records created in the transaction of public business

Adherence with the recommendations laid out in this document will support more efficient document retrieval, mitigate the loss of public records due to inaccessibility, and improve the agency's ability to respond to public records and e-discovery requests.

What is SharePoint?

SharePoint is part of a suite of software tools offered by Microsoft Corporation. It functions as a collaboration tool that combines several functions, including: intranet, extranet, content management, document management, personal cloud, enterprise social networking and search, business intelligence, workflow management, and web content management. In addition, SharePoint provides central management, governance, and security controls for content management and collaboration. Although it does some records management capabilities, it is not intended to be used as records management tool for long term records.

SharePoint is a browser-based tool that provides communication and collaboration tools to improve productivity and efficiency in the government workforce. Within SharePoint users can store, track, and manage electronic documents and assets. Additional tools include:

- Versioning — SharePoint allows some versioning of documents by allowing them to be "checked in" and "checked out" and will manage the versions of the document so that users are aware of the most up-to-date version.
- Collaboration — SharePoint enables users to collaborate in real time using the live collaboration and editing tools, thus reducing the need to generate and manage emails.
- Synchronized files — Because it is centrally hosted, SharePoint can synchronize files across devices.
- Rights Management — SharePoint site administrators can set user permissions (i.e., read, write, modify, access).
- Search — SharePoint allows users to search across sites and configure the results to display information they wish to see—all, by format, by date—and allows the user to define how the results to be displayed in different ways—grid, detailed, filtered, etc.
- Updated software — In a hosted instance, the software is updated independent of users and users content and sites are upgraded automatically so that content is accessible regardless of the software used to originally create it.
- Ability to "tag" files — SharePoint provides tools to allow users to "tag" documents utilizing a taxonomy developed by the site users. The tagging feature makes it easier to search and retrieve documents.

What is OneDrive for Business?

OneDrive for Business is "personal online storage space in the cloud, provided for you by your company. Use it to store your work files across multiple devices with ease and security. Share your files with business colleagues as needed, and edit Office documents together in real time with Office Online. Sync files to your local computer using the OneDrive for Business sync app."[1]

Employee Responsibilities

Do not solely store records on SharePoint or OneDrive for Business

G.S. § 132 defines a public record as "all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, artifacts or other documentary materials, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions."[2] Regardless of where records reside,

[1] OneDrive for Business Service Description. (2015). Retrieved September 10, 2015, from https://technet.microsoft.com/en-us/library/onedrive-for-business-service-description.aspx

[2] "§ 132-1.2. Confidential Information." Chapter 132. Public Records. North Carolina General Assembly, 2014. Web. 10 August. 2015. <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>.

they are still public records and employees must manage them according to their records retention and disposition schedule. For more information regarding records management, please refer to the state agency and local government retention and disposition schedules, available at **https://archives.ncdcr.gov/government/retention-schedules**. By statute, records that relate to public business are public records and employees must manage them as such. In particular, OneDrive for Business accounts are tied specifically to an individual employee's authenticated authorized account and, therefore, is not accessible to other employees or IT professionals; employees may not store public records solely on OneDrive for Business. Employees must also save records to networked storage or in a repository.

Manage Records Appropriately

Employees are responsible for managing their records appropriately. SharePoint and OneDrive are collaboration tools, but they are not a records management tool and do not have the robust capabilities to assign retention or disposition of records. SharePoint does, however, have capabilities that permit users to add information and "tag" or categorize their files. The tagging feature allows people to create categories for records, it may be that a short-term record is assigned a numerical tag. For instance, records retained for two years and then destroyed may be given a tag that reads "2 year_2016." Employees who use this schema will know that record needs to be kept for two years and can be destroyed in 2016. Users could also use the tagging features to link the record to the series item number found in the functional schedule for state agency records or the group to whom it belongs, e.g. "dncr." A simple place to start is to tag documents or files as "permanent" or "archives" if they have that disposition according to the Records Retention and Disposition schedule.

Employees are responsible for managing their sites and documents, and ensuring the records are managed properly. If your agency has a records management software tool, official records should be moved or checked into that software tool (e.g. Documentum Records Management, OpenText, or TRIM) or moved to a shared drive. This is especially critical for users of Office365.

Records in SharePoint need to be actively managed in accordance with the records retention schedule. When new versions of a record are loaded into a SharePoint, older versions need to be evaluated according to the records retention and disposition schedule. If the documents are drafts and the new document replaces the former document, you may delete the prior draft. If records are scheduled to transfer to the State Archives, please contact your records management analyst. For information regarding transfer, please refer to our guidance documents to prepare your records for transfer. Records exported from SharePoint should be exported along with the metadata associated with the record. The metadata and the document together comprise the "official record."

OneDrive for Business enables employees to remotely access records and documents. Once records are ready for review or collaboration, employees must move them from OneDrive for Business to networked shared storage, into a repository, or into a collaboration tool such as SharePoint. OneDrive for Business is not intended for permanent storage of public records.

Important note: OneDrive for Business is tied to the account activated for a state agency employee. In order for this account to be created, the employee must be authenticated and authorized. For Microsoft services, the account is an employee's e-mail address and NCID password. Because it is the entire email address, each agency has a specific domain within OneDrive for Business; therefore, stored documents will not transfer when an employee moves from one state agency to another. When an employee leaves an agency (even if transferring to another agency), the employee must transfer documents and files from OneDrive for Business and make them accessible by a supervisor on shared network storage. When the user account is deleted, so is the content associated with that OneDrive for Business account. For this reason, Human Resource Directors and employees' supervisors must ensure that migrating files out of OneDrive for Business becomes part of the mandatory exit process when an employee leaves the agency.

Information Technology staff are a critical support piece for records management. DNCR encourages employees to communicate their storage needs to IT in order to properly manage the records and ensure the appropriate

management of information assets. DNCR strongly recommends that agencies form an Information Governance Committee to set policies regarding how and where records are stored and managed. At a minimum, the members of that committee should consist of information technology staff, the chief records officer, the records manager (if applicable), as well as a high level executive sponsor or manager.

Protect Sensitive and Confidential Information

Keep confidential information off SharePoint and OneDrive for Business. Confidential data includes information that if accessed by unauthorized entities could cause personal or institutional financial loss or constitute a violation of statute, act, or law. Records that are subject to confidentiality restrictions include:

- Personal identifiable information such as library record that identifies a person as having requested or obtained specific materials or service
- Confidential communications by legal counsel to public board or agency, state tax information, public enterprise billing information , or records associated with the Address Confidentiality Program, as well as documents related to the federal government's process to determine closure or realignment of military installations
- Trade secrets or information disclosed or "furnished to a public agency in connection with the owner's performance of a public contract or in connection with a bid, application, proposal…."
- Login/password credentials
- Those that reveal "the electronically captured image of an individual's signature date of birth, driver's license number or a portion of an individual's social security number"
- Those that reveal the seal of a licensed design professional
- State Employee Personnel files (with the exception of certain information that can be disclosed).
- Protected health information (PHI) in any form or medium created or received by a health care provider, health plan, employer or clearinghouse. PHI is defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as health information "that identifies the individual" or "with respect to which there is a reasonable basis to believe the information can be used to identify the individual."[3] The Public Health Law of North Carolina also stipulates the confidentiality of "privileged patient medical information" in the possession of DHHS or local health departments.
- Student records protected by the Family Educational Rights and Privacy Act of 1974 (FERPA).

Confidential information should be stored on local resources that are appropriately secured.

Tools Related to OneDrive for Business and SharePoint

There are several tools within Office365 that interact with OneDrive for Business and SharePoint. It is important to remember that all materials shared in these tools are subject to public records law, and should therefore be used in a manner in accordance with the above guidelines.

Teams

Microsoft Teams is an instant messaging and remote meeting tool. Teams stores chats and shared files in OneDrive for Business and SharePoint, depending on the nature of the interaction; private chats are stored in the user's OneDrive, while Team channels are stored in SharePoint. The conversation history and Teams chats are recorded in users' inboxes and are discoverable in eDiscovery, depending on the agency parameters.

[3] HIPAA 'Protected Health Information': What Does PHI Include? (2015). Retrieved September 9, 2015, from https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

Stream

Microsoft Stream is a video sharing software. It stores recorded Teams video meetings and calls, as well as uploading and sharing videos, and live streaming events. Videos shared in Stream are stored in SharePoint, and storage is based on DIT-set retention periods. Stream also creates transcriptions for discovery of video in eDiscovery.

Delve

Microsoft Delve is a layer on SharePoint that operates much like Pinterest, based on the search index in SharePoint. The graphic user interface (GUI) shows the user all of the files that they have access to, and displays how many times the user has viewed the document. It is a secure access layer that will not change existing permissions of a file set by the file's owner.

Education and Training

Employees are responsible for their own records and bear full responsibility for SharePoint and OneDrive for Business management. It is crucial that they understand their responsibilities as users of SharePoint and OneDrive for Business and custodians of the public record. We strongly encourage agencies to train new employees on proper electronic records file management and naming. More information regarding records management and public records can be found at **https://archives.ncdcr.gov/government**. More information about handling digital files can be found at **https://archives.ncdcr.gov/government/digital-records**. Online tutorials are available at **https://archives.ncdcr.gov/government/records-management-services-and-training/online-tutorials**. Additionally, staff from the State Archives are happy to assist with training and workshops for staff to help them set up and manage their public records.

Summary

- SharePoint is a browser-based tool that provides communication and collaboration tools to improve productivity and efficiency in the government workforce.
- OneDrive for Business is a personal online storage space in the cloud, provided for employees using Office365. Materials/files stored in this space can be accessed across multiple devices with ease and security.
- Digital records require active management by the records creators. SharePoint and OneDrive for Business are not intended for permanent storage of public records.
- Employees must move public records from SharePoint and OneDrive for Business to networked shared storage, or into a repository.