OneDrive for Business: Best Practices and Usage

April 2020
Version 2.0

State Archives of North Carolina
NATURAL AND CULTURAL RESOURCES

Contents

Purpose

Upon employment, government employees typically receive access to shared storage, as well as a drive dedicated to them and their user profile. A "personal" drive provides employees with a place to store documents that are still in progress, but not are quite ready for sharing or distribution. This drive provides storage for employees while also enabling IT to provide backup and recovery services. Typically, this drive is simply part of centralized network file storage and is not accessible outside the network without the capability to login remotely using a virtual private network.

Executive Agencies and the Department of Information Technology have purchased Microsoft's Office 365 (O365) subscription services. Office 365 designates subscription plans that include access to Office applications plus other productivity services available via the Internet (thereby also known as cloud services). One element of this subscription available to state employees in North Carolina is OneDrive for Business. Although Microsoft offers different levels of service in O365 subscriptions, this document refers specifically to OneDrive for Business.

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

- Definition of OneDrive for Business
- Purpose of OneDrive for Business
- Use of OneDrive for Business by public service employees
- 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 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]

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,*

[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

available at **https://archives.ncdcr.gov/documents/best-practices-cloud-computing-records-management-considerations**.

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.

Employee Responsibilities

1. Do not solely store records on 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, 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. Because the OneDrive for Business account is 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.

2. Manage Records Appropriately

Employees are responsible for managing their records appropriately. 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

[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>.

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 must ensure that migrating files out of OneDrive for Business becomes part of the mandatory exit process when an employee leaves the agency.

3. Protect Sensitive and Confidential Information

Keep confidential information off 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….[3]
- 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[4]
- 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…."[5]
- Login/password credentials[6]
- 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"[7]
- Those that reveal the seal of a licensed design professional[8]
- State Employee Personnel files (with the exception of certain information that can be disclosed).[9]

---

[3] Confidentiality of library user records. (1985). Retrieved September 9, 2015, from http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=125

[4] "Confidential Communications by Legal Counsel to Public Board or Agency; State Tax Information; Public Enterprise Billing Information; Address Confidentiality Program Information." Chapter 132. Public Records. North Carolina General Assembly, 1995. Web. 9 Sept. 2015. <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>.

[5] "Confidential Communications by Legal Counsel to Public Board or Agency; State Tax Information; Public Enterprise Billing Information; Address Confidentiality Program Information." Chapter 132. Public Records. North Carolina General Assembly, 1995. Web. 9 Sept. 2015. <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>.

[6] Inspection and Examination of Public Records. (2014). Retrieved September 9, 2015, from http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132

[7] § 132-1.2. Confidential information. (2014). Retrieved September 10, 2015, from http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132

[8] § 132-1.2. Confidential information. (2014). Retrieved September 10, 2015, from http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132

[9] Chapter 126. North Carolina Human Resources Act. (2014). Retrieved September 9, 2015, from http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=126

- 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."[10] 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.[11]
- Student records protected by the Family Educational Rights and Privacy Act of 1974 (FERPA).[12]

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

Education and Training

Employees are responsible for their own records and bear full responsibility for OneDrive for Business management. It is crucial that they understand their responsibilities as users of 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**. 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

- 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. Employees' OneDrive for Business is not intended for permanent storage of public records.
- Employees must move public records from OneDrive for Business to networked shared storage, into a repository, or into a collaboration tool such as SharePoint.

---

[10] 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/

[11] "Chapter 130A. Public Health." § 130A-12. Access to Health Information. North Carolina General Assembly, 1983. Web. 9 Sept. 2015. <http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=130A>.

[12] "Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99." U.S. Department of Education. U.S. Department of Education, 26 June 2015. Web. 9 Sept. 2015. <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.