



Indiana Office of Technology

Powering a State that Works

OneDrive for Business

Employee/Agency Usage and Responsibilities

Policy Number: Operations (ITP) 16-01

Effective Date: 04/21/2016

1. Purpose

Upon employment, all employees, including contractors, are given a home 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 home drive provides storage for employees while also enabling the Indiana Office of Technology to provide backup and recovery services. Typically, this drive is simply part of centralized network file storage and is not accessible outside the network unless accessed using virtual private network.

The Indiana Office of Technology has purchased SharePoint Online subscription services for a number of agencies. One element of this subscription is OneDrive for Business. Although Microsoft offers different levels of service in O365 subscriptions, this document refers specifically to OneDrive for Business.

OneDrive for Consumer is a separate service offered by Microsoft to the general public. At no time is OneDrive for Consumer supported by the Indiana Office of Technology.

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.

2. Revision History

Revision Date	Revision Number	Change Made	Reviser
04	01	Policy Origination	S. Kremer

3. Persons, Groups, Systems Affected

All agencies within the Executive Branch of Indiana State Government and those connected to the Statebackbone.

4. 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 Microsoft owned servers located in data centers located in the continental United States. Storing files remotely is sometimes referred to as Cloud Storage. Please refer to agencies policy as it pertains to cloud storage and management of cloud storage.

OneDrive for business allows employees to make changes from different devices, even if they do not have the software installed. OneDrive is similar to other services like, Dropbox or Google Drive. However, OneDrive for business is an IOT approved solution to use with state data and provides employees the ability to access this data from multiple devices and locations. Unlike DropBox or Google Drive, OneDrive for Business is accessed by only authenticated users with accounts issued by the Indiana Office of Technology. It is important to remember, any document stored on OneDrive for Business will become inaccessible and unrecoverable 30 days after an employee leaves or transfers to another agency. An email will be sent to the manager when the SharePoint/OneDrive account has been closed and they have full access to the data for 30 days. It is the responsibility of the manager and the agency to determine what data needs to be kept, and then place it in an appropriate place.

5. Folder and File Sharing

OneDrive for Business is a personal online storage space hosted at a Microsoft datacenter. A feature in OneDrive for Business allows easy sharing of files and folders with employees and potentially people outside the organization. Below is a list of recommendations by the Indiana Office of Technology on how to share files in folders.

- Use folders to share group files with other employees
- To protect your agency from data spillage, only share with specific individuals; never everyone, or 'public'.
- Use caution when sending links to shared folders. Links, like an attachment, can be forwarded. Recipients may not realize the sender doesn't want others to access the information, or they may not realize they are sharing it.
- Warning: Anyone you have shared a file or folder with can share it with others.
- It is the agencies responsibility to review sharing privileges every quarter and removes these privileges when they are no longer needed.

6. Responsibilities

6.1. Employee and Agency Responsibilities

Regardless where documents reside they are still considered public records and employees must manage them according to your agencies record and retentions policies set by the IARA. Your agencies specific records and retention schedules are available at http://www.in.gov/apps/iara/retention/iara_retention. Since OneDrive business is tied to a specific individual employees authenticated account, therefore by default it is not accessible to IOT or other employees, employees should not use OneDrive for Business to solely store public records. Employees should also save records to the provided network attached storage or another repository solution.

Employees are responsible for adhering to retention policies and managing their data appropriately. OneDrive for Business is not intended to be used a permanent storage of public records. When a document is ready for review or shared, they must be moved to SharePoint Online, Network shared storage, or another type of repository.

Agencies are responsible for the data that will be stored on OneDrive for business. Keep all confidential information off of OneDrive for Business. Confidential data accessed by unauthorized entities could cause personal or institutional financial loss or constitute a violation of a statute, act, or law. Please refer your agencies compliance director to determine what data might be seen as confidential.

6.2. IOT Support and Responsibilities

IOT, at this time, can only provide limited support of OneDrive for Business. Since OneDrive for business is an add-on to SharePoint online it was never intended to

replace our fully support solution of Syncplicity. It is the agencies responsibility to identify issues and test functionality before allowing employees to utilize OneDrive for Business. IOT support responsibilities are as follows:

- Installation of client.
- Allowing users, the ability to reach OneDrive for Business from State provided desktop or Laptop.
- Support is limited to the integration with SharePoint Online.
- IOT is not responsible for security patches that might be applied that break OneDrive for Business. The agency will need to notify IOT if they believe a security patch may interfere with OneDrive for Business.
- IOT reserves the right to disable OneDrive for Business at any time if they determine the OneDrive for Business has been compromised or cannot comply with security requirements defined by IOT's security policies.