Service Policy

Cloud Document Storage: OneDrive

Responsible Executive: Chief Information Officer, WCM
Original Issued: June 11, 2018
Last Updated: September 8, 2021

Contents
1. What is OneDrive? ................................................................. 2
2. Eligibility for OneDrive ........................................................... 2
3. Acceptable Data to Store in OneDrive ...................................... 2
4. Accessing Data in OneDrive ................................................... 2
5. Sharing and Collaboration ....................................................... 2
6. OneDrive Data and Departure from WCM ................................. 2
7. Auditing of OneDrive Accounts ............................................ 2

1. What is OneDrive?

OneDrive is a cloud document storage service provided by Microsoft. It allows users to store, access, and share files through the cloud. OneDrive is available for Microsoft Office 365 subscribers and can be used on various devices, including Windows, Mac, Android, and iOS.

2. Eligibility for OneDrive

Eligibility for OneDrive is based on the user’s role and department within WCM. Employees, contractors, and partners who are approved by WCM leadership for access to OneDrive can use the service.

3. Acceptable Data to Store in OneDrive

Data that is approved for storage in OneDrive includes documents, presentations, spreadsheets, and other types of files that are part of the user's work responsibilities and are necessary for their job functions.

4. Accessing Data in OneDrive

To access OneDrive, users need to log in to the OneDrive website or use the OneDrive app on their device. Once logged in, users can browse and manage their files and folders, upload new files, and download or delete existing files.

5. Sharing and Collaboration

OneDrive supports sharing and collaboration through the sharing feature. Users can share files and folders with other users, granting them read, write, or edit permissions. Collaboration features, such as real-time editing and comments, are also available.

6. OneDrive Data and Departure from WCM

When an employee departs from WCM, their OneDrive account should be reviewed to ensure that sensitive data is properly archived or deleted. The responsible executive should follow the data retention policy and guidelines for the appropriate handling of data.

7. Auditing of OneDrive Accounts

Auditing of OneDrive accounts is performed periodically to ensure compliance with data protection regulations and to monitor for any unauthorized access or activity. Audits may include reviewing file access logs, monitoring for unusual activity, and performing regular backups for data protection.

This document is intended to provide guidelines for using OneDrive within WCM. Questions or concerns about using OneDrive should be directed to the responsible executive or the IT department.
1. What is OneDrive?
OneDrive is an enterprise cloud storage solution included as part of Office 365 and allows WCM users to store electronic files in one place and collaborate with others. OneDrive enables real-time editing and collaboration tools within the Microsoft Office suite to update documents in one convenient and secure space. Documents stored in OneDrive can be shared among other OneDrive users.

2. Eligibility for OneDrive
OneDrive is offered with Weill Cornell Medicine email (Office 365) accounts.

3. Acceptable Data to Store in OneDrive
In accordance with ITS policy 11.03 – Data Classification, Weill Cornell Medicine classifies data into three risk categories: high, moderate, and low. Unlike other cloud document storage solutions, OneDrive may be used to store high risk data in addition to moderate and low risk data.

4. Accessing Data in OneDrive
OneDrive can be accessed via any web browser by going to https://portal.office.com. You may log in using your WCM CWID and password and clicking the OneDrive tile. OneDrive offers mobile applications and sync clients; however, offline file synchronization is only permitted on encrypted devices which are tagged and managed by ITS.

5. Sharing and Collaboration
A prominent feature of OneDrive is the ability to share documents with others and collaborate in real-time. Sharing data is permitted between internal users, WCM affiliates (as maintained on the WCM website at https://weill.cornell.edu/our-story/affiliations), or sponsored guests (external, non-affiliated users). However, to maintain an audit trail, sharing must be with a named account (i.e., no sharing with an anonymous link).

6. OneDrive Data and Departure from WCM
If users leave WCM, they will no longer have access to their OneDrive account. Any personal documents should be migrated out of the OneDrive account prior to leaving the institution. Any documents pertaining to WCM or developed for WCM purposes cannot be removed.

7. Auditing of OneDrive Accounts
To ensure compliance with this policy, ITS will randomly audit OneDrive accounts and scan the contents with our data loss prevention (DLP) software. Any high risk data files identified to be shared beyond a minimum necessary or with anonymous users will have their sharing permissions reduced in accordance with this policy.