Office 365: OneDrive Security Recommendations

Last Modified on 05/27/2021 2:11 pm CDT

Microsoft OneDrive for Business (known at UW-Eau Claire as OneDrive –UW-Eau Claire and hereafter in this document for simplicity's sake as OneDrive), is secure cloud-based storage. Microsoft has guaranteed (via our contract or their web site) the data is stored within servers in the U.S., data is encrypted in transit and at rest, and customer data will not be accessed for uses other than troubleshooting or as directed by users. (See the Office 365 Trust Center for more information.) However, because OneDrive is a cloud-based file storage and sharing utility, its use presents some potential risk to UW-Eau Claire and its students, faculty, and staff:

- Data stored in the cloud can be accessed by any workstation, laptop, tablet, or mobile device with access to the Internet.
- Students, faculty, and staff are likely to access data in a variety of ways, including potentially unsecured connections from off-campus locations. It is not possible for UW-Eau Claire to govern how OneDrive is being accessed by non-university computers or Internet connections.
- With OneDrive UW-Eau Claire has no ability to monitor how individuals set up security/file sharing. It is possible someone could accidentally share files to the world.
- When files are shared with others or synchronized and stored locally from a device that is infected with viruses or malware, the data is likely to be compromised as well.

Content

Appropriate File Storage on OneDrive

UW-Eau Claire offers a variety of storage options designed to handle particular needs that may arise. Some options may be more appropriate for specific types of files based on their content and size.

- Information protected under the following security standards is considered confidential and should NOT be stored on OneDrive (and, really, copies should not be stored anywhere outside of the databases in which this data resides):

    - FERPA –academic information, including grades (more information at http://www.uwec.edu/Registrar/student/privacy.htm).
    - HIPAA and PHI –healthcare information.
    - PCI –credit card and other financial information.

- Non-protected information may be stored and shared in OneDrive, but must be stored and shared in a secure manner (see suggestions for How to Use OneDrive Securely below).
- Storage limits are quite high, but maximum individual file sizes, upload/download transmission times, and file synchronization times may discourage some extremely large files from being stored in OneDrive.
- The LTS Digital Data Storage Tool provides multiple alternatives for specialized file storage.

How to Use OneDrive Securely

Secure the workstation or device you are using to access OneDrive:

- Install virus/malware detection software with the latest definitions.
- Run a firewall that blocks in-bound traffic.
- Do not log into your workstation or device as an administrator (unless absolutely necessary).
- Keep your operating system and software up-to-date.
- Password-protect your workstation or device and use idle-time screen saver passwords where possible.
- Talk to your departmental IT support for help securing your computers and other devices.

Use only secure network connections:

- Use the UW-Eau Claire wired network or the uwec.edu WiFi when on campus.
- Implement the FTC's best practices for using public WiFi connections.
- Implement the FTC's best practices for securing home wireless networks.

Exercise caution when sharing files online:

- Sharing files with the default "Can edit" permission level allows the person you shared that file with to further share the file. If you would like to change this behavior see the page on enabling access requests.
- Pay attention! It is very easy to accidentally share the wrong folder or to share a folder rather

than an individual file within a folder. Remember that the default for sharing is "Can edit", but it can be changed to "Can view".

- Use folders to share groups of files with others online.
- Share files with specific individuals, never with "everyone" or the "public".
- Remember that the delivered **Shared with Everyone** folder means what it says: it is **Shared with EVERYONE**! (Office 365 makes it very easy to find documents, even if they are stored in someone else's OneDrive!)
- Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.
- Remember that once a file is shared with someone and they download it to their device, they can share it with others.

Review sharing privileges in OneDrive on at least a quarterly basis:

- Remove individuals when they no longer require access to files or folders.

University of Wisconsin-Eau Claire