OneDrive Security and Use Guidelines

Revised: 4/9/2024

OneDrive for Business is Microsoft's cloud-based file storage service, for work or school. OneDrive lets you store, share and collaborate on files.

OneDrive provides 1TB of storage space and allows you to access them from anywhere, and share files with other users.

Our data is stored on Microsoft servers located in the U.S., and data is encrypted. However, because OneDrive is a cloud-based file storage and sharing utility, its use presents some potential risk to GNTC and its students, faculty, and staff:

- Data stored in the cloud can be accessed by any computer, 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 GNTC to govern how OneDrive is being accessed by non-GNTC computers or Internet connections
- GNTC has no ability to monitor how individuals set up security/file sharing. It is possible someone could accidentally share files to the world. So, it is extremely important to follow these guidelines to keep your OneDrive as secure as possible
- 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

Appropriate File Storage on OneDrive

- Information protected under the following security standards is considered confidential and should **not** be stored on OneDrive without consultation and specific approval from Technology Services:
    - FERPA –academic information, including grades, SSNs, and Student ID #s
    - 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
- Storage limits are quite high, but maximum individual file sizes, upload/download transmission times, and file synchronization times may discourage extremely large files from being stored in OneDrive.

How to Use OneDrive Securely

Secure the computer or device you are using to access OneDrive.

While we do many of these steps for you when using GNTC computers on campus, these are things that you should look into when teleworking or using non-GNTC devices.

- Install anti-virus/malware software and keep up-to-date with the latest definition updates.
- Run a firewall that blocks in-bound traffic
- Do not log into your computer or device using the main administrator account
- Keep your operating system and software up-to-date

- Password-protect your computer or device and use idle-time screen saver passwords where possible. Remember to lock your computer when you step away.
- Use only secure network connections:
  ○ Use the GNTC wired network or the GNTC 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:

- The default option for a shared file is 'Can Edit'. Sharing files with the default permission level allows the person you shared that file with to further share and edit the file, unless you change the permissions to 'Can View'
- Accidentally sharing the wrong folder or to share a folder rather than an individual file within a folder is easy to do so pay attention to what you are sharing. 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 easy to find documents, even if they are stored in someone else's OneDrive
- Be careful sending links to shared folders because they can 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

Request File with One Drive

With the file request feature in OneDrive, you can choose a folder where others can upload files using a link that you send them. The users that you request files from cannot see what is in the folder - they can only upload files to it.

- Anyone can send you a file - they do not need to have OneDrive
- All the files sent to you are saved in a single folder that you choose
- It is recommended that you use a different folder for each 'type' of file that you are requesting
- People who respond to your request can only upload files. They do not have view or edit access to your OneDrive

How-To Steps

1. In OneDrive, select or create a folder that you want others to upload to. Click the three dots at the end of the folder name. Select 'Request files' from the menu
2. Under 'What files are you requesting?' enter a descriptive name for the files that you are requesting for others. (It is very important that you provide a good description of the type of file that you are expecting here.) Click Next.
3. You can then enter an email address or addresses to that you wish to receive a file from if they are using a GNTC faculty/staff/student email. You also have the option to add a message here. Otherwise, you will need to send an email with the link copied and pasted into an email. Click 'Done'.

You will receive an email notification; however, this notification may be delayed based upon the Microsoft network. If you want to edit the descriptive name of the file request, select the folder and click 'Request

files' again, then change the name. The people you sent the request to will see the new name when they upload files.

Review sharing privileges in OneDrive

It is important to regularly review your sharing privileges in OneDrive. Review privileges on at least a quarterly basis and remove individuals when they no longer require access to files or folders.

Have issues?

If you have questions or any additional issues, please submit a Support Request, and someone from Technology Services will be happy to assist you.