CLOUD STORAGE OF INSTITUTIONAL DATA: USE GUIDELINES

UW Tacoma Information Technology offers faculty and staff multiple tools for sharing and saving work-related files, such as the H: and S: drive, Microsoft OneDrive, and Google Drive. Although OneDrive and Google Drive are endorsed as an approved sharing solution for the campus, there are some guidelines to follow to ensure the services are being used properly. Additionally, you should check with your department's leadership to ensure they support the use of cloud storage.

WHEN NOT TO USE CLOUD STORAGE (GOOGLE DRIVE, MICROSOFT ONEDRIVE)

Google Drive and Microsoft One Drive are both UW-approved storage providers. They both offer storage and remote sharing capability with other users in UW. While convenient, there are some items that you may want to consider storing on the S: drive. Some examples are:

- Files that are commonly used by others in your department, or used by others around campus.
- Files that are critical to the function of your department

Should the person who shares the file decide to depart UW Tacoma, the files located in their cloud storage will no longer be available for use. If the files are placed on the S: drive, they can continue to be used long after their departure.

WHAT INFORMATION CAN BE SAVED IN CLOUD STORAGE

The University of Washington has an agreement with both Google and Microsoft that allows FERPA-protected information to be stored in these systems. Additionally, the agreement with Microsoft extends to HIPAA-protected data. The University of Washington does not have such an agreement in place with Google, so it is recommended that Google not be used to house HIPAA protected data. Certain precautions should be taken when storing this type of data in the cloud since it can be readily accessed by multiple devices, some without proper protections. For more information, please refer to the File Sharing Services matrix.

HOW TO USE MICROSOFT ONEDRIVE AND GOOGLE DRIVE SECURELY

Secure all computers or devices you intend to use to access these services by:

- Installing virus/malware detection software that is up-to-date, with the latest definitions.
- Keep your operating system and software up-to-date.
- Password-protect your workstation or device. Log off or lock your workstation or device when stepping away.
- Do not sync files to a machine or device that is not issued and/or secured by UW Tacoma IT.
- Do not store personal files in these services.
- Share files with specific individuals, never with "everyone" or the "public".

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

RECORDS RETENTION IN THE CLOUD

As a state agency, everything created both in hardcopy and electronic form is considered a record, and no record may be destroyed unless it's retention period is approved by the State Records Committee. Data stored in the cloud is subject to the same retention schedule rules – please check the retention schedules to determine how long your data should be stored. Once the data has exceeded the required retention period, the record may need to be destroyed. Refer to the Destroying Records guide posted by Records Management Services.

OTHER CLOUD STORAGE PROVIDERS

If you or your department are considering the use of a cloud storage company not outlined above, it is best to consult with the Information Technology department before doing so, as there may be compliance or security-related issues that would need to be addressed before initiating the purchase. A list of common storage providers can be found on the File Sharing Services Matrix.

Note: Individuals or departments considering using Canvas should note that storage in Canvas is intended only for purposes directly related to group and coursework.