TAMUK SECURE DATA STORAGE

Data Storage Options

TAMUK ITS currently offers 5 different types or levels of data storage to all Faculty and Staff members.

These options include :

- Redirected Documents – Individual User Storage – TAMUK Internal Users Only
- Departmental Shared Drive – Multi User Shared Storage – TAMUK Internal Users Only
- Microsoft One Drive – Multi User Shared Storage – Both Internal and External Users
- TAMU Syncplicity – Multi User Shared Storage – Any TAMU Syncplicity User
- TAMUK Data Center SAN – High Speed Physical Storage – TAMUK Internal Users Only

Note that you are not limited to a single option when contemplating your options for the safe & secure storage of critical data. You can choose from any of the options individually or you can choose to utilize all 5 options. Your choice(s) will be largely dependent on the features and limitations of each platform. The Descriptions for each option are detailed below.

Redirected Documents

A Personal Storage Space, also known as The Redirected Documents Folder, is available for all faculty and staff users. This drive will serve as a safe and secure option for storing your data instead of storing data either on the PC or on some type of external drive.

Use of the Redirected Documents Folder will substantially lessen the chance of lost data due to a PC failure or external Drive Failure.

This drive can be requested by calling the ITS Help Desk at x4357. ITS will process the request, set up the Drive and verify that it is working. Once completed users can then migrate all of the files that are typically maintained on a PC Hard Drive or External Storage Device by simply moving them into the “Documents” Folder.

- The Redirected Documents storage solution is provided free of charge to all TAMUK Faculty & Staff.
- The initial size of the Redirected Documents Folder is 100 gigabytes. Size increases are available based on capacity and demand.
- Requests for increased space can be made via the Helpdesk by and should include an estimate of the amount of additional space needed.
- The Redirected Documents Folder is only available to TAMUK faculty and staff.
- The Redirected Documents Folder is intended to be used for data storage only, not applications. It is recommended that you keep external copies (Cd, DVD, etc) of critical applications for cases that might require a complete rebuild of your PC.

- Files such as music and personal files that are not for TAMUK business use should not be stored on your Redirected Documents Folder.
- The Redirected Documents Folder is only accessible by the named user and has no sharing capabilities.
- The Redirected Documents Folder does not provide encrypted data storage so it is recommended that it not be used for the storage of "sensitive" (PCI, HIPPA, FERPA) data.
- To significantly reduce the risk of data loss your Redirected Documents Folder is backed up to magnetic tape each week and is also replicated in real time to our alternate Data Center at TAMU in San Antonio. Weekly Tape Backups are kept both in a secure location on site and also to a safe deposit box at a local bank in Kingsville.
- To have your personal Redirected Documents storage set up – Please contact the ITS Help Desk at x4357(HELP) to put in a request and ITS will take it from there.

Departmental Shared Drive

A Departmental Shared Drive is a common network drive that can be utilized for storing files and data that needs to be accessed and maintained by multiple users. Each Departmental Shared Drive will have a designated Shared Drive Manager. The Shared Drive Manager will be provided an easy to use utility program that will allow him or her to manage the group of persons that have access to the share.

- The Departmental Shared Drive storage solution is provided free of charge to all TAMUK Faculty & Staff.
- The initial size of the Departmental Shared Drive is 50 gigabytes. Size increases will be available based on demand and available capacity.
- Requests for increased space can be made via the Helpdesk by the share manager and should include an estimate of the amount of additional space needed.
- Departmental Shared Drives are only available to faculty and staff groups and are typically used for institutional departments or projects.
- Student-workers may be granted limited access for the specific work assigned to them, but the department share manager is responsible for maintaining data security and access for each student.
- Any department that needs to store sensitive data should contact ITS so that a secure encrypted drive solution can be set up for that department.
- Network shared drives are for file and data storage, not applications. Files such as music and personal files that are not for TAMUK business use should not be stored on Departmental Shared Drives..
- The Departmental Shared Drive is not intended as a place to back-up a user's personal data files from a TAMUK computer. See the information on the "Redirected Documents Folder" for that type of space.
- To significantly reduce the risk of data loss the Departmental Shared Drive is backed up to magnetic tape each week and is also replicated in real time to our alternate Data Center at TAMU in San Antonio. Weekly Tape Backups are kept both in a secure location on site and also to a safe deposit box at a local bank in Kingsville.

To request a new Departmental Shared Drive contact the ITS Helpdesk at x4357 to have a ticket opened for you. Along with the request, let us know who the initial users are and who the designated Share Manger will be so we can set up that access when creating the drive. You will be notified when the shared drive is operational.

Requests to add or remove users from the group list of a Departmental Shared Drive will be handled by the designated Share Manager. Usernames are required to correctly identify the user. Note that existing users who leave the institution or have their role status changed will not be automatically removed from your list of users who have access by ITS; so it will be the Share Manager's responsibility to manage such events.

One Drive Cloud Storage

Included with our campus Microsoft Agreement is OneDrive Cloud Storage. Files stored here can be accessed from anywhere with an internet connection. Additional Information on setting up and using the TAMUK implementation of OneDrive can be found here:

Click Here for One Drive Video Trainings

On the "Video Trainings" website you can also sign in to your Office 365 Account by clicking on "Sign In" at the top of the page. Remember to use your "ku" username when signing into Office 365 – for example: kuabc123@tamuk.edu.

- The Microsoft One Drive storage solution is provided free of charge to all TAMUK Faculty & Staff and Students.
- By default, One Drive currently provides 1 Terabyte of Cloud Storage space for Faculty, Staff, and Registered Students. The capacity can be increased to 5 Terabytes on request. To request a capacity increase, contact the ITS Helpdesk at x4357 to have a ticket opened for you
- OneDrive does what all the other cloud storage services do — it gives you a place to put your files on the Internet. You need to log in to OneDrive with your Microsoft account to access your data.
- You can share files or folders that are stored in OneDrive by sending or posting a link to the file or folder to whomever you want. OneDrive creates a link for you that you can email to whomever needs access.. You can also specify whether a file or folder is Public or Private so you have complete control over who has access to what.
- To work with the OneDrive platform on a mobile device, you can download and install one of the OneDrive programs — OneDrive for Mac, OneDrive for iPhone, iPad, or Android.
- In Windows 10, you don't need to download or install a special program for OneDrive — it is already built in to Windows.
- OneDrive syncs data among computers, phones, and/or tablets that are set up using the same Microsoft account, as soon as you connect to a network. If you change a OneDrive file on your iPad, for example, when you save it, the modified file is put in your OneDrive storage area on the Internet. From there, the new version of the file is available to all other computers with access to the file.

One Drive provides many enhanced security features to protect your data. These features include:

- **Virus scanning on download for known threats** - The Windows Defender anti-malware engine scans documents at download time for content matching an AV signature (updated hourly).

- **Suspicious activity monitoring** - To prevent unauthorized access to your account, OneDrive monitors for and blocks suspicious sign-in attempts. Additionally, we'll send you an email notification if we detect unusual activity, such as an attempt to sign in from a new device or location.

- **Ransomware detection and recovery** - As a Microsoft Office 365 subscriber, you will get alerted if OneDrive detects a ransomware or malicious attack. You'll be able to easily recover your files to a point in time before they were affected, up to 30 days after the attack. You can also restore your entire OneDrive for up to 30 days after a malicious attack or other types of data loss, such as file corruption, or accidental deletes and edits.

- **Version history for all file types** - In the case of unwanted edits or accidental deletes, you can restore deleted files from the OneDrive recycle bin or restore a previous version of a file in OneDrive.

- **Password protected & expiring sharing links** - As an Office 365 subscriber, you can keep your shared files more secure by requiring a password to access them or by setting an expiration date on the sharing link.

- **Mass file deletion notification and recovery** - If you accidentally or intentionally delete a large number of files, we will alert you and provide you with steps to recover those files.

- **Secure Data Encryption** - All data stored in the One Drive Cloud is encrypted.

- **One thing to note** - Microsoft One Drive Cloud (and all other Cloud Storage options) – upload and download speeds for your data is completely dependent upon the bandwidth (speed) of your internet connection. For this reason, Cloud Storage may not be the best choice if you need to store Application Data in the cloud and then process that data with an application residing on your PC. It is most suitable for simply the storage and encryption of large amounts of data that you would normally access by downloading from the cloud back to your PC.

Your Microsoft One Drive storage solution is already set up – You can login to One Drive by going to https://onedrive.live.com/about/en-us/signin/

Remember to use your "ku" username when signing into One Drive – example: kuabc123@tamuk.edu

Please contact the ITS Help Desk at x4357(HELP) if you need any assistance with One Drive.

Syncplicity – A&M Cloud Storage

Syncplicity offers a secure cloud environment for all users in The Texas A&M University System to store and share documents with any other person. For other users within the A&M System that also have Syncplicity - you can share your entire Syncplicity Directory. For persons external to the A&M System – you can create a link to your files and share them by sending that link to anyone with an email address. Additionally, you can access all of your files from anywhere with an internet connection. Additional Information on setting up and using the TAMUK implementation of Syncplicity can be found here:

Overview of Syncplicity Functionality

Sharing a Folder in Syncplicity

Online Instructions for Using Syncplicity

- **Cost of Storage** - The Syncplicity Cloud Storage solution is currently provided free of charge to all TAMUK Faculty & Staff through an agreement with TAMU College Station.

- **File Sharing –** Files and Folders set up in Syncplicity can be shared with other Faculty or Staff member within the Texas A&M University System.

- **Accessibility** - Syncplicity offers users the ability to sync any folder or desktop, include or exclude subfolders, and it can be used on nearly any platform utilizing a Syncplicity Client application for Mac, Windows, iOS and Android.

- **Storage capacity** is currently advertised as "virtually unlimited" (although I don't know that has been tested) which makes it a great option for the storage and sharing of multiple terabytes of data and files.

- **Secure Data Encryption** - All data stored in the Syncplicity Cloud is encrypted.

- **One thing to note** - Syncplicity Cloud (and all other Cloud Storage options) - upload and download speeds for your data is completely dependent upon the speed of your internet connection. For this reason, Cloud Storage may not be the best choice if you need to store Application Data in the cloud and access that data with an application on your PC. It is most suitable for simply the storage and encryption of large amounts of data.

TAMUK Data Center – Storage Area Network (SAN)

Brand New Option - ITS has recently brought online a 500 Terabyte Storage Area Network device, or SAN, in the College Hall Data Center. This was purchased and implemented with the intention of providing a solution for those Faculty, Researchers, and Departments that require high speed access and high levels of data integrity for large amounts of locally stored data.

The Data Center SAN solution is a high end solution that removes the bottlenecks associated with Cloud Solutions for users connected via the TAMUK Network. Additional characteristics of the TAMUK Data Center SAN Solution are as follows:

- The TAMUK Data Center SAN option is a cost per Terabyte option which will need to be charged back to your Department Budget Account. Note that your cost per Terabyte is an annual fee with a "true up" at the end of each year. Note that the costs associated with this option go to pay for the Hardware, Software, and Engineering needed to maintain the system and is not designed to be a profit center for ITS. It is recommended that this option be used for data that you absolutely cannot afford to lose. Please contact ITS for cost estimates if you need this type of storage.

- User Access and Functionality appears very similar to TAMUK Department Shares including the ability to grant local access to other TAMUK Users. File and Folder access is NOT available to Non TAMUK Users.

- The TAMUK SAN solution does not currently provide encrypted data storage so It is recommended that it not be used for the storage of "sensitive" (PCI, HIPPA, FERPA) data. Please contact ITS if you need encrypted data storage.

- Accessible from Off-Campus through the TAMUK Global Protect VPN Portal.

- The fastest reading and writing option for local users on the TAMUK Network.

- Real Time Data Replication to our alternate Data Center at TAMUSA provides a simple and very effective Disaster Recovery solution. In the event of a catastrophic failure at the TAMUK Data Center the remote TAMUSA Data Center (with an exact replica of your data) can be brought online very quickly.

- To significantly reduce the risk of data loss ALL SAN data is backed up to magnetic tape each week. Weekly Tape Backups are on a rotating weekly schedule and are kept both in a secure location on site and also in a safe deposit box at a local bank in Kingsville.

- To schedule an appointment to discuss TAMUK Data Center SAN Storage - Please contact the ITS Help Desk at x4357(HELP) to put in a request and ITS will take it from there.