



# Texas Wesleyan University

## Information & Communication Technology

### **Shared Drive Policy**

This document defines policies and procedures for storing, maintaining, and controlling data on university shared drives.

#### **Policy**

TW wishes to ensure that each school and department is able to efficiently access, update, and share school/departmental documents and mission-critical and mission-essential data. The shared drive provides a secure location to store shared school/departmental documents and data.

All documents and data required for the day-to-day, short-term, and long-term operation of the school or department should be stored on the shared drive. Additionally, any document or data that is being used by two or more individuals in the school/department toward the achievement of the school/department mission may be stored on the shared drive.

#### **Eligibility**

All TW academic and administrative departments and schools are eligible.

#### **Requirements**

Shared drives are set up for each university department and school automatically. Departmental Supervisors or School Deans may request that specific members of the department/school be provided access to a shared drive by completing the Shared Account Request Form (available online at the ICT Web site).

#### **Shared Drive Maintenance**

It is the responsibility of the School Dean (school shared drives) or Departmental Supervisor (department shared drives) to stay within their allotment of disk space, ensure that all mission-critical and mission-essential documents and data are stored on the shared drive, and to archive older document versions.

#### **Shared Drive Backups**

Data on the shared drive will be regularly backed up by the ICT department using the standard Server Backup procedure and timeline.

#### **Data/Document Management**

To ensure that the proper version of information is located on the shared drive, that all mission-critical and mission-essential data and documents are stored on the shared drive (and not on an employee's PC or H: drive), and that employees are able to efficiently access all necessary school/departmental data and documents, the following document management strategies should be followed:

1. Each school/department must establish and follow a review process to ensure that documents/data to be placed on the shared drive are timely, accurate, and appropriate.
2. A master list should be kept that tracks all documents/data stored on the shared drive.
3. It is recommended that the folder structure be based upon the services, activities, or functions of the school/department. Folders can be created for each major service, activity, or function the school/department performs. The folder name should describe its contents (e.g. this document could be located inside the "Policies" folder).
4. All documents should include a descriptive file name and date of last modification (e.g. this policy document could be named "shared\_drive\_policy\_033106"). The file name would indicate that this is the Shared Drive Policy and it was last modified on March 31, 2006.
5. The Departmental Supervisor or School Dean should appoint someone to regularly (once per year) audit the shared drive to ensure that all appropriate documents/data are being stored on the shared drive and that the appropriate employees are able to gain access.
6. Invalid or obsolete documents/data must be removed immediately when identified. Prior drafts and multiple copies of documents should not be stored on the shared drive.
7. Updates to documents posted on the shared drive should be approved by the Departmental Supervisor or School Dean before being carried out.