Texas A&M AgriLife Research Procedures

29.01.99.A0.02 │ Enterprise File Service

Approved: December 15, 2011
Revised: September 12, 2014

Next Scheduled Review: September 12, 2019

PROCEDURE STATEMENT

This procedure establishes enterprise file services standard operating procedures for all of Texas A&M AgriLife Research (AgriLife Research) positions.

REASON FOR PROCEDURE

The Texas A&M AgriLife Extension Service (AgriLife Extension), AgriLife Research, and the Texas A&M University (TAMU) College of Agriculture and Life Sciences have deployed a state–wide enterprise file storage service. The purposes of this document are to outline features and service levels, and to establish formal guidelines and procedures related to the use of the service. These procedures are established to achieve the following:

- ensure compliance with applicable statutes, regulations, and rules regarding data retention and management;

- define required practices regarding the use of enterprise file services; and

- educate individuals who may use enterprise file services with respect to their responsibilities associated with such use.

PROCEDURES AND RESPONSIBILITIES

1.0   GENERAL

    1.1   Terms of use:

        Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of AgriLife Research are the property of the agency.

    1.2   Violation of these procedures may result in termination of employment or other business relationships existing between the agency and individual. Additionally, individuals are subject to loss of access privileges for AgriLife Research information resources, and potentially civil or criminal prosecution.

    1.3   Any exceptions to the procedures outlined must be preapproved by the director of AgriLife Research.

2.0   ENTERPRISE FILE SERVICE DESCRIPTION

    2.1   The enterprise file service was established to facilitate the following needs:

        A.   secure data storage for business operation files;

        B.   automated off–site data backup to meet system policies; and

        C.   ease of access and enhanced collaboration for employees.

    2.2   Key features of the enterprise file service include the following:

A. *File and Folder Versioning*—This feature allows users to recall on average up to 64 previous copies of a file or directory of files. This feature is performed by checking files and folders each hour from 8:00 a.m. to 6:00 p.m. on workdays for any changes. If a change is detected, a new version of the file is created and is accessible by right–clicking on the file for access and retrieval. See the *AgriLife End User Enterprise File Services Guide* for more details.

B. *Near Real–Time Off–site Data Replication*—This feature copies data from department enterprise file servers securely to the AgriLife core data center located in Bryan/College Station. As required by state policy, this feature facilitates off–site data backup allowing for automated data replication and information technology (IT) regulation compliancy.

C. *Quota Management*—Quotas are provided to assist users in managing their enterprise file server storage status.

D. *Usage Reports*—Department IT managers have access to automated usage reports to assist in management of data storage by individual users.

3.0 ENTERPRISE FILE SERVICE MANAGEMENT AND OPERATION MODEL

The enterprise file service is managed and maintained centrally by the AgriLife IT unit with respect to hardware maintenance, system upgrades, and monitoring. For departments and locations that have a dedicated IT manager, tasks such as user access, quota, and workgroup directory management can be delegated.

Department IT managers can read more detail about this operating model by accessing the *AgriLife Enterprise File Server Management Guide*.

4.0 SERVICE LEVEL PARAMETERS

4.1 There are two key service–level elements within the enterprise file service. The following is a description and details regarding the service or operating levels associated with each.

A. *File/Directory Versioning*—File/directory versioning is a service that allows users to quickly recover deleted or previous versions of a file or folder. This is performed by a right–click on a file or folder to access the "*Previous Versions*" tab. From this tab, users can access any available versions of a folder or file for instant retrieval. See the *AgriLife End user Enterprise File Services Guide* for more details.

- The versioning recovery feature should optimally be considered to recover versions of files or directories 1 to 3 days past.

- Versions (or snapshots) of directories and their files are taken every hour on weekdays from 8:00 a.m. to 6:00 p.m. Any file created and deleted within the hour will not have a version created and is not recoverable.

- Versioning is not to be considered or relied upon as a robust backup feature.

B. *Backup Tape Restoration & Retention Service*—Enterprise server file data is replicated in near real–time to a secured core storage system located in Bryan/College Station. From this location, an enterprise tape system performs data backup on a nightly basis. The following table depicts restoration availability for files at any given time.

Time Frame	Files that can be Restored from Backup*
Last 30 Days	Any file from any weekday can be restored*
1 Month to 3 Months	Any file that existed on any Friday*
4 Months to 12 Months	Any file that existed on any last weekday of the month*
1 Year to 2 Year	Any file that existed the last weekday of the year*

Note: The file must have existed on the file server during the time that nightly backups are performed (10:00 p.m. to 5:00 a.m.) in order to be recoverable.

The following presents the various types of tape backups performed and what timeframes each are retained. Each of these schedules was formally initiated on 12/11/11.

- Daily Backups—Each night of the week (Monday – Thursday) incremental backups are made of all files and directories that have changed since the previous backup. Incremental daily backups will be maintained for up to 1 month.

- Weekly Backups—Weekly backups are conducted each Friday evening, and perform a full backup of all the data. Full backups will be maintained for up to 12 weeks.

- Monthly Backups—Monthly backups are full backups that are made on the last weekday of each calendar month. Monthly backups are retained up to 11 months.

- Yearly Backups—Yearly backups are made on the last weekday of the year. Yearly backups will be retained up to 2 years.

Note: Any files considered original state records requiring retention should be stored in the AgriLife Laserfiche system for compliancy with state, System and agency records retention requirements.

4.2   Examples of files that cannot be retrieved are:

A.   A file that was created 4 months ago on a Monday, and then was deleted on a Thursday of the same week. This file would not be retrievable as it would not exist on either of the weekly or monthly tapes.

B.   A file that was created 1.5 years ago, but deleted before the end of the calendar year. This file would not be retrievable as it did not exist on the file server at the end of the calendar year.

C.   A file created and deleted 1.5 months ago that did not exist on any Friday during that month.

D.   A file that was created and deleted during any weekday, but did not exist at the beginning of any hour between 8:00 a.m. and 6:00 p.m. This file would not have existed during one of the hourly file version snapshot routines.

5.0   END USER RESPONSIBILITIES

5.1   Data Recovery Requests

Employees should specify via a FirstCall help desk request (first-call@tamu.edu) the following information when requesting recovery of a deleted file or directory of files:

A.   full employee name;

B.   departmental affiliation and/or location;

C.   file name(s) and/or directory path to be recovered;

D.   date file was deleted (if known); and

E.   date of the file or directory to recover.

5.2   Personal Data Files

At no time shall enterprise file server space be utilized for storage of non–business related data. Any incidental use of personal data should only be performed on a local workstation. Examples of personal data include non–business related music files, photos, gaming software, files containing personal financial information.

5.3   Full Workstation Backups

A. Full workstation backups shall not be stored on the enterprise file server. This creates an undue burden and cost to the off–site replication process as full workstation backups contain temporary files and large application installations.

B. Full workstation backups shall be performed through local devices (i.e. USB Hard drives) connected to workstations, or through other local departmental resources.

5.4 Application Software

Application software shall not be installed on an enterprise file server. Only data files of application software shall be stored for backup and off–site replication.

5.5 Temporary Large Scale Storage

Enterprise file servers should not be utilized for large scale temporary data storage unless performed and approved by a department IT manager or AgriLife IT. Large scale temporary storage negatively impacts the off–site data replication process. Contact your department IT representative or AgriLife IT before performing this type of activity.

5.6 Workstation Data Accountability

Each employee is accountable for data stored on their local workstations. Only data stored on the enterprise file servers will be backed up and protected off–site, unless alternative solutions are provided within a department. There are several methods for both manually and automatically placing data on the enterprise file servers. They include:

A. Use the enterprise file server as your default storage space vs. your local hard drive. This can be accomplished by saving directly to a network drive or having an IT staff member redirect (Windows OS Only) your local "My Documents" folder to the file server. This is recommended for all users with non–portable workstations.

B. Utilize replication software to automatically copy data from your local hard drive data directory to the enterprise file server. This method is highly recommended for users that utilize laptops for their computer workstations. Contact AgriLife IT or your department IT manager for suggested software solutions.

C. Manually copy data from your local hard drive to the enterprise file server on a regular basis. This is the least recommended model as it does not adequately protect your data should your local hard drive fail between copies.

5.7 Quotas

Quotas have been deployed on enterprise file servers to allow for oversight and management of space usage per user. The purpose of quotas is to promote proper maintenance of data files.

A. A 10GB quota is set by default for all employees for personal directory space. Requests for increases should be sent to the FirstCall helpdesk or department IT staff where applicable.

B. Automatic email notifications are sent to both the employee and department IT manager (or AgriLife IT) when 85%, 95%, and 100% of quota is obtained.

5.8 File Locking and Sustained File Open Connections

Some application software performs a feature called "file locking" that prohibits other users from deleting or changing a file while it is in use. This feature—while beneficial to protecting a file—does create an issue for file replication and versioning. When a file is in use with activated "file locking," a version of the file and a copy of the file cannot be made to the off–site storage location.

Additionally, users who have files opened from a network file server for prolonged periods of time (with or without file locking) are susceptible to data loss should there be a network outage or failure of the enterprise file server.

As both of these situations result in limited or no ability to restore or recover a data file, it is recommended that users practice the following guidelines:

A.   When using an application that performs file locking, close the application when not in use to optimize version creation and off–site replication of the associated data files.

B.   When required to use an application for a prolonged period of time (i.e. a data collection software tool), utilization of a local workstation hard drive is recommended to limit exposure of data loss from any network or file server outage.

6.0   IT MANAGER RESPONSIBILITIES AND GUIDELINES

Department authorized IT managers should be familiar with the *AgriLife Enterprise File Server Management Guide.* Responsibilities and guidelines are as follows:

6.1   User Personal Folder Naming Convention

A.   User personal folders will be created centrally through the AgriLife IT onboarding process.

B.   All user personal folders will be named in the form of "firstname.lastname" with lower case lettering for consistency purposes.

6.2   Drive Mapping Conventions

If drive mapping is used within a unit or center, the following standard drive letter mappings shall be utilized. These drive mappings are automatically created through active directory scripting.

A.   P: Drive shall be configured in the Windows Remote Administration Server Tool for each user, and be directed to each individual user's personal directory.

B.   S: Drive should be mapped to the "\share" directory for the employee's designated file server.

C.   W: Drive should be mapped to the "\group" directory for the employee's designated file server.

6.3   Share Directory Management (S: Drive)

Department IT managers are responsible for managing the use and upkeep of the S: drive for their allocated enterprise file server. This directory should be used for public sharing of information within the department, and should also be routinely managed to remove outdated or unused data files. Department IT managers are responsible for performing regular maintenance and oversight of this directory in coordination with department employees.

6.4   Temp Directory Management

A.   The temp directory should be used to store large "evergreen" data such as ISOs. Additionally, this space could be used for temporary large scale data storage (i.e. moving data from one workstation to another) as the temp directory is not included in the network replication routine.

B.   The temp directory is not replicated or backed up. Should an enterprise file server be impacted by a failure event (i.e. flood or fire), any data in the temp directory will be lost.

6.5   Enterprise File Server Storage Upgrade Request and Review Process

AgriLife IT and department IT managers (where applicable) receive automated alerts when any enterprise file server reaches 95% of total storage capacity. When this quota is obtained, it is the responsibility of the

department IT manager to perform the following process. If a department IT manager does not exist, then AgriLife IT will perform the analysis.

The analysis consists of the following steps:

A.   Perform an analysis of the data storage being used on the system by running and analyzing reports offered by the File Server Resource Manager application.

B.   Remediate with users any data that may be removed or that is not allowed for storage on the enterprise file server.

C.   Contact AgriLife IT to provide a summary of the analysis stating whether or not there is a need for further review, and assess the need for increasing available storage capacity for the server.

D.   AgriLife IT in partnership with the department will assess the recommendation, and discuss appropriate next steps.

E.   Enterprise server storage capacity will not be automatically increased until a formal review has been formed on existing data storage and a recommendation for increase has been requested by the associated department.

6.6   Local Folder Redirection to Enterprise File Servers

For workstations with Windows 7 operating system (and above), redirection of certain local folders (i.e. My Documents, Favorites, etc.) is allowed to other locations (i.e. a network file server). This technique allows for users to have local folders and files stored automatically on a server without the need of 3rd party software or a manual process. The following procedures must be followed when applying local folder redirection:

A.   Local Folder redirection shall only be targeted to a folder within a user's personal (P: Drive) directory. It shall not be targeted directly to the personal folder itself.

B.   Local Folder redirection shall not be applied to laptops, and only be utilized for non–mobile desktop computers.

6.7   Assist in Local On–Site Environment and Security Management

A.   Assist AgriLife IT in managing on–site electrical power and UPS maintenance.

B.   Assist in managing physical security controls and procedures.

C.   Assist in managing air handling systems status and management.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

AgriLife Research Procedure 29.01.03.A0.01 *Information Resource Procedures*

AgriLife Research Procedure 61.99.01.A1.01 *Retention of State Records*

AgriLife End User Enterprise File Services Guide

AgriLife Enterprise File Server Management Guide

CONTACT OFFICE

For questions, contact AgriLife Information Technology at 979-845-9689.