

# Shared Drive Policy

Approved October 10, 2008  
by Chief Information Officer Dwight Fischer

## 1.0 Purpose

The purpose of this policy is to establish standards for creation and maintenance of shared file services at PSU.

## 2.0 Scope

This policy applies to all file services hosted on ITS central file servers.

## 3.0 Policy

### 3.1 Ownership and Responsibilities

A Shared Network Drive is a common network folder that can be utilized for storing files that need to be viewed / maintained by multiple users. Generally the folder sharing is among users in a particular department, but can be extended across departments. One or two users must be designated as "manager" of the share. With such rights, the manager has the responsibility for maintaining who has access to the share. Thus, the manager is responsible for notifying ITS to provide access to new users and removing those who no longer should have access.

### 3.2 Use

- ITS provides secure, backed-up shared network drives for the purpose of storing data used for institutional business.
- Requests for increased space must be made via the Helpdesk by the share manager and should include an estimate of the amount of space needed.
- Quota increases are available based on capacity.
- Before quota increases are granted, ITS reserves the right to inventory drive contents and suggest alternatives such as archival, compression, reorganization or removal of unused content.
- Shared file areas are only available when accessed through a secured private network or via PSU's VPN.
- Shared drives are only available to faculty and staff groups typically for institutional departments or projects.
- Student-workers may be granted limited access for the specific work assigned to them, but the department and/or share manager is responsible for maintaining data security.
- Any department that needs to store sensitive data on a shared drive needs to provide written justification to the Chief Security Officer (CSO) or designee.
- Network shared drives are for data storage, not applications.

- Files such as music and personal files (ie. photo's, resume's etc..) that are not for PSU business should not be placed on shared drives.
- The shared drive is not intended as a place to backup a desktop computer.
- Users are expected to do their own restores of deleted or damaged files using "Previous Versions" before initiating a request to have it restored from a historical backup; for more information please contact the Helpdesk (x52929).

### **3.3 Establishing a network drive**

To request a new shared network drive:

- A statement of need and purpose or request for additional space.
- An estimate for the initial size and expected growth rate and length of need  
Identification of the shared drive manager(s)
- Backup requirements.

### **3.4 User Access**

Requests to add or remove users from the access list of a shared drive needs to be initiated by the designated share manager via the Helpdesk. Usernames are required to correctly identify the user. Users who leave the institution or have their role status changed may not be automatically removed from share access by ITS; it is the managers responsibility to inform ITS in a timely manner.

### **3.5 Compliance**

- Audits will be performed on a regular basis by ITS.
- Audits will be managed by the internal audit group or ITS, in accordance with the Audit Policy. ITS will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

### **4.0 Shared document areas not maintained by ITS**

It is possible to share documents either directly from a PC or special purpose network device. ITS recommends caution when establishing shared file areas not supported under the central infrastructure. The department or individual assumes full responsibility for user access, data loss, data security and backups. For a list of approved shared device strategies, contact the Help Desk at the Learning Commons ([helpdesk@plymouth.edu](mailto:helpdesk@plymouth.edu)).

### **5.0 Enforcement**

Any share may be, at the discretion of the CSO or designee, removed or disabled, if it is found to be in violation of PSU and USNH policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 5.0 Definitions

Term	Definition
CSO	Chief Security Officer.
Server	For purposes of this policy, a Server is defined as an internal PSU machine providing services for a group of people or other machines. Desktop machines and Lab equipment are not relevant to the scope of this policy unless it is providing services to other people or machines.
Fileshare	A shared storage area on the server used to facilitate group activities.