

# Old Dominion University Computer Science Department Policies and Procedures

**Title: Sensitive Data Storage**

**ID: CSD001**

**Revision: 1.0**

## **Purpose**

The purpose of this document is to define the policy accepted by the Computer Science Department in regards of the storage and protection of sensitive data.

## **Scope**

This procedure pertains to all members of the Computer Science Department.

## **Policy**

Responsibility for the handling of data storage is left to the discretion of the owner. Each guest, student, faculty or staff member is required to store sensitive data on pre-defined storage locations provided by Systems Group. Data stored on each of the predefined shared storage locations will be properly encrypted and backed up on a regular basis. Backup guidelines are specified in Data Backup Procedures CSB001.

- Student Storage Locations

Undergraduate, Graduate, and PhD students must save any sensitive data in their student share. To access that location, the individual can use a CIFS share (Z-drive) on Windows, or their respective home directory on UNIX. Any sensitive data must not be stored on default Windows profiles.

- Guest Storage Locations

Guest of the Computer Science Department must save any sensitive data in their account share. To access that location, the individual can use a CIFS share (Z-drive) on Windows, or their respective home directory on UNIX. Any data stored on default Windows profiles will be deleted immediately after the termination of a Windows login session, both physical and remote.

- Faculty/Staff Storage Locations

Faculty and staff members must save any sensitive data in their respective share. To access that location, the individual can use a CIFS share (Z-drive) on Windows, or their respective home directory on UNIX. Any sensitive data must not be stored on default Windows profiles. Files utilized during the collaboration of staff and faculty members may also be stored on the CIFS share on server storm.cs.odu.edu.

- Research Storage Locations

The data utilized during the collaboration of faculty and student members on a specific project, must be stored in a pre-defined research data location. Each faculty members is responsible for requesting such a storage share and maintaining a current list of members to have access to the share. To access that location, the involved parties will be provided with the path to a CIFS share on Windows, and a respective NFS share on UNIX. All sensitive data must not be stored on the defined storage location.

The department of Computer Science recognizes the existence of data storage on mobile devices. Such include, but are not limited to, USB drives, cell phones, personal digital assistants, and digital music players owned by faculty, staff, students and guests. The department prohibits the storage of sensitive data on devices not owned by the Computer Science Department. In case the person has been allocated such a device, the owner is responsible for protecting the data. This includes both encrypting and backing it up. All sensitive data must be encrypted according to the guidelines in the Computer Science Department Data Encryption policy CSD002. The Department requires that each owner of such a device returns it to Systems Group for proper data removal and sanitizing.

## Definitions

NFS: Network File System. A type of shared file systems utilized on various Operating Systems providing access to a shared file storage location over the network.

CIFS: Common Internet File System. A type of shared file systems utilized on Windows and Linux Operating Systems providing access to a shared file storage location over the network.

## Revision History

1/7/2011 – Rev 1.0 Pending approval by Ajay Gupta