Augsburg College Information Technology Backup Policy

I. Overview

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers.

II. Purpose

The purpose of this backup and recovery policy is to provide for the continuity, restoration and recovery of critical data and systems in the event of an equipment failure, intentional destruction of data, or disaster.

III. Scope

The Department of Information Technology is responsible for the backup of data held in central systems and related databases. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the college falls entirely to the user. Campus users should consult their Liaison for Computing or the Student TechDesk about securing locally stored data.

The disaster recovery section of this policy apply to all Network Managers, System Administrators, and Application Administrators who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

IV. Definitions

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

V. Schedule

Full backups are performed weekly on Friday evenings. If, for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday. Incremental backups are performed Monday through Thursday or Saturday through Thursday.

A monthly full backup set shall be made using on the first weekend of every month.

Operating system files and application files that are not user created may be backed up on weekly basis as long as installation media is available.

VI. Retention

Full backups are retained for a minimum of two months. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.

Incremental backups are retained for one week or until the next full backup has been made.

Monthly full backups are retained for one year.

VII. Responsibility

The Director of Information Technology Systems shall delegate a member of the IT Department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

VIII. Testing

The ability to restore data from backups shall be tested at least once per month.

IX. Data Backed Up

Data to be backed up includes the following information:

- User created data
- Databases (system and user)
- Application and Operating System Files
- System state data
- Registry (Windows systems)
- Etc directory (Linux systems)
- Active Directory and eDirectory

All IT managed servers and storage, such as networked attached storage devices, are required to be backed up.

XII. Restoration

Users that need files restored must submit a request to their Liaison for Computing or the Student TechDesk. Required information include: the name of the file, creation date, the last time it was changed, and the date and time it was deleted or destroyed.

Requests for the restoration of all or parts of campus databases shall be forwarded to the Director of Information Technology Systems.

XIII. Tape Storage Locations

Tapes used for full backup shall be stored in the Science Building in the vault.