Data Backup Policy

Summary

Tape backups are critical to safeguarding the applications and data stored on CSU's network. Backups are necessary to recover from events such as natural disasters, system disk drive failures, data entry errors, or system operations errors. It is important to clarify that data backups provide for restoring data that is lost unexpectedly – we cannot rely on backups for archival purposes.

Purpose

The purpose of this policy is to set forth principles, procedures, and responsibilities for data backups, including the responsibility that users have regarding their own data.

Policy

- Daily backup of all user data, application data, and critical applications *stored on network file servers* is mandatory. Full system backups are preferred.
- Due to limited time and media resources, system backups do not include data stored on personal computers.
- If a user accidentally loses networked data, UITS will make a reasonable recovery effort.
- No less than three backup cycles shall be maintained. One cycle will be in use, one cycle will be stored in a fireproof cabinet on site, and one cycle will be stored in a fireproof cabinet off site.
- The backup media retention period is three weeks.
- Documentation, periodic review, and testing of the backup and recovery process are required.
- Media must be physically destroyed before being disposed.

Procedures and Responsibilities

- UITS personnel, typically systems administrators, are responsible for all system backup and restore activity on CSU file servers.
- University Police transport tapes off site each week.
- The Information Security Officer initiates testing of restores on critical servers at least once a month.
- Every computer user is responsible for maintaining adequate backup copies of critical or irreplaceable data. UITS recommends that users store their data on the network in their home directory (H: drive). In some cases, storing files on the network and having them backed up to tape is sufficient. In other cases,

users may want to maintain a separate copy on their hard drive, a CD, DVD, or the like.

Related USG Policy

5.10 (IT Handbook) Required Reporting & 9.4 (IT Handbook) Data Access

Last Update

2/4/2014

Responsible Authority

Chief Information Security Officer