Recommendations
for Protecting Vital Data
for Disaster Recovery Purposes

Disasters come in many forms, e.g., earthquakes, water damage, computer viruses and major power outages. It is essential to protect vital campus records and data. Vital data is being defined as sensitive or confidential information relating to student academic records, fiscal data, personnel information, and records required for the effective management of the University, such as Executive Memoranda and disaster recovery plans.

If vital information is stored on a computer's hard drive that becomes infected with a virus or the computer is damaged as a result of an earthquake, important data could be lost completely. Data stored on paper can be ruined by fire or water damage from flooding or leaking. If the original and a back-up copy are stored in the same area and a disaster occurs in that area, both could be lost.

The following recommendations are made, based on the survey results, to ensure that vital records can be recovered after a disaster.

- Use surge protectors to guard against data loss due to power surges.

- Back up vital data to a separate medium.

  Examples of media used for storing data: hard drive (c:), floppy disk, paper, magnetic tape, jaz drive, network storage available through a software program such as Legato

- Back up vital or confidential data at least weekly.

- Store the back-up copy in a separate location from the original.

  For example, if the original is stored on the computer's hard drive, save the back-up copy on a floppy disk or paper and store it in a separate office or building.

- Ensure that backed-up data can be read at the separate location.

  For example: Compatible software (correct versions of Microsoft Word, Excel, Access, Power Point, etc.) should be available at the separate location to read data stored on a portable magnetic medium, i.e., floppy disk, tape or jaz drive.