# Disaster Recovery
# Information Security Procedure

**Basis for Procedure**

6051 Computer Use and Electronic Information Security Policy

**1. Purpose**

1.1. The purpose of this plan is to outline procedures to respond to an emergency or other occurrence (for example, fire, vandalism, system failure and other natural disasters) that damages systems that containing electronic confidential information.

**2. Definitions**

1. *Disaster Recovery Plan* (DRP) is a written plan that details how to prevent the things that can be prevented and recovering from the things that cannot be prevented. Recommended items to be included:
   1.1. Personnel Contact List
   1.2. Vendor contact List
   1.3. Equipment and specifications
2. *Downtime Procedures* are the processes which will be followed if the computer information system is not available. Downtime procedures identify the activities, resources, and procedures needed to carry out the processing requirements during prolonged interruptions to normal operations. This would include but is not limited to utilizing paper, utilizing a different computer system or other means to ensure continuity of operations.

**3. Authorities and Administration**

3.1. Assistant Vice Chancellor, Information Technology Services
3.2. Information Security Officer

**4. Procedure**

4.1. It is the responsibility of the information custodian to ensure that procedures are in place to create and maintain retrievable exact copies of confidential information. The information custodian/system administrator is responsible for determining the back up medium, backup medium rotation schedule and if the backups should be stored off site.

4.2. The information custodian/system administrator is responsible for developing a disaster recovery plan which establishes procedures to restore any loss of data.

4.3. The information custodian is responsible for ensuring that there is a plan to maximize confidentiality of information and to maintain operations in the event of a disaster (downtime procedures). This plan would include emergency mode operations.

4.4. The information custodian will test components of the Disaster Recovery Plan periodically. The outcome of the test should be documented. A sample form (Attachment A) may be used for documentation of the test. The Disaster Recovery Plan should be updated as issues are identified by the testing. Documentation of the testing should be maintained in departmental files.

**Attachment A**
**Disaster Record Test Scenario Worksheet**
**(Name of Event)**

| | |
|---|---|
| Date, Time, Place | |
| Purpose of test | |
| Expected outcome | |
| Type of test (Circle one) | |
| Section of DR to be tested | |
| Duration of test | |
| Timeline of events | |
| Assumptions to be used | |
| Data to be restored/entered | |
| Equipment to be restored | |
| Actions taken | |
| Persons responsible | |
| Outcome | |
| Recommendations | . |