

# ACU Technology Disaster Preparedness and Recovery Plan

*Written: February 1995*

*Last updated: February 2007*

**ACU employee information is available only when viewed at ACU.**

---

## Acknowledgments

We gratefully acknowledge the help and ideas taken from the following disaster recovery plans:

*Baylor University Center for Computing and Information Systems Disaster Recovery Plan CSD0247, CAUSE, Baylor University, May 25, 1988.*

The Baylor plan also acknowledged the following plans:

*Disaster Recovery Plan CSD0093, CAUSE, Appalachian State University, February 4, 1982.*

*Disaster Recovery Plan CSD0139, CAUSE, Colorado State University, January, 1983.*

*Off-Site Processing Plan CSD0143, CAUSE, The San Diego Community College, September 6, 1983*

*The Data Center Disaster Consultant, 2nd ed., Kenniston W. Lord, Jr., Q.E.D. Information Sciences, September, 1981.*

## Purpose and Scope

### Introduction

Abilene Christian University (ACU) has set up a highly computerized operational environment. This includes the use of microcomputers in offices as well as servers that provide much of the operational support for the administrative and academic units. A campus-wide network ties these various systems together and provides communications to other computer networks, universities, and the computer diagnostic facilities of selected computer vendors involved. In addition, the operation of the campus network provides a vital support component of the university system, including the operation of local and long distance telephone services and cable TV.

The reliability of computers and computer-based systems has increased dramatically. Computer failures that do occur can normally be diagnosed automatically and repaired promptly using both local and remote diagnostic facilities. Many computer systems contain redundant parts, which improve their reliability and provide continual operation when some failures occur. In years past, most computer operations were predominantly batch-oriented. Disaster plans were comprised primarily of reciprocal agreements made between users of similar systems for job processing (usually at night and/or weekends). This has become less feasible with the very complicated on-line and diverse network systems most institutions now have installed. Although institutions may have similar equipment and operating systems, they generally do not

have the capacity to add a large number of users from another on-line environment to their systems even if the technical problems could be solved.

Another possibility is to find alternate sites near the local systems where any additional equipment needed can be shipped in rapidly, and critical on-line operations for the organization can be resumed in a reasonable time. Redundancy in the communications network and a tie-in to the alternate site, or the ability to rapidly tie-in, is an important part of the disaster plan. This type of site is called a cold backup site, as opposed to a hot backup site which contains all equipment necessary to start immediate operations.

For the most part, the major problems that can cause a computing system to be inoperable for a length of time result from environmental problems related to the computing systems. The various situations or incidents that can disable, partially or completely, or impair support of ACU's computing facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require special funding from the university in order to allow the affected systems to be repaired or replaced. This report assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery.

### **Objectives/Constraints**

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the central site or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting different departments in ACU's technology areas. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the university, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the computing support given to ACU clients from academic and administrative systems under the stewardship of ACU technology areas. The elements that concern microcomputers are addressed; however, client-related functions not directly tied to computer and telephone support by ACU technology areas are not addressed. Also, offices at ACU should develop their own plan to deal with manual operations within their office should computer and/or network services be disrupted. Due to cost factors and benefit considerations at this time, the alternatives of hot sites and contracts with disaster recovery companies are considered infeasible and unnecessary for ACU.

All major computing systems that are vital for the daily operation of the University and under the stewardship of ACU technology areas are maintained under service contracts with the

equipment vendors. This ensures that routine maintenance problems will be addressed in a timely way with adequate resources. These contracts range from telephone support only to full hardware replacement.

## **Assumptions**

This section contains some general assumptions, but does not include all special situations that can occur. Any special decisions for situations not covered in this plan needed at the time of an incident will be made by senior technology staff members on site.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first one on site following an incident will contact the CIO for a determination of the need to declare an incident. The CIO will determine who else needs to be notified including when to notify the Vice President for Finance.

The senior technology staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured. The ACU Department of Public Safety and Physical Plant will be notified if necessary. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., **but** evacuation is the highest priority.

Once an incident which is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper university authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable technology and/or telephone support to the university has been re-established.

## **Incidents Requiring Action**

This disaster recovery plan for ACU will be invoked under any of the following circumstances:

- An incident which has disabled or will disable, partially or completely, the central computing facilities, and/or the communications network for a period of 24 hours.
- An incident which has impaired the use of computers and networks managed by ACU technology areas due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all academic and administrative systems which ACU technology areas manage. This includes, but is not limited to, hardware failure, internet attacks, virus attacks, and spam attacks.
- An incident which was caused by problems with computers and/or networks managed by ACU technology areas and has resulted in the injury of one or more persons at ACU.

## **Contingencies**

General situations that can destroy or interrupt technology and telephone services usually occur under the following major categories:

- Power/Air Conditioning Interruption
- Fire
- Water
- Weather and Natural Phenomenon
- Sabotage and Interdiction

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- Partial recovery - operating at an alternate site on campus and/or other client areas on campus.
- Full recovery - operating at the current central site and client areas, possibly with a degraded level of service for a period of time.

### **Physical Safeguards**

#### **Zellner Hall**

Zellner Hall is protected by an electronic door lock on the west exterior entrance. All Zellner employees have access through this reader using their ACU ID card. Keys to other exterior doors are restricted to selected personnel. (Who has keys??)

There is an electronic door lock on each of the entrances (one a Diebold and one with a TESA lock) to Zellner 119, telecommunications equipment room.

There are electronic locks on the entrances to Zellner 300 and Zellner 310 (TESA lock). A combination lock exists on the entrance to Zellner 307 from the east stairwell. Only technology employees who need regular access have the combination. There is a bypass key on the combination lock on the east stairwell door. The Associate CIO has this key.

#### **Zellner 119 - Telecommunications Equipment Room**

This room houses the telephone switch, voice mail system, cable television equipment, and data communications equipment. It is the hub for each of these campus-wide data, voice, and video networks. There is no protection against water damage.

The telephone equipment is connected to a 48V DC UPS system. This will maintain the telephone switch for 3 hours. Other equipment in this room is connected to individual or clustered UPS equipment. This equipment room is protected by a fire protection system using FM200. ZE119 also houses the main DMARC for the campus and the primary distribution point for fiber and copper for the campus.

#### **Zellner 310 - computer room**

Zellner 310 houses centralized computing equipment for Information Services.

All three rooms are covered by one, eight-zone halon fire protection system which requires positive signals from two of the zones to discharge. The rooms have been sealed to prevent leakage during discharge. System Administrators have been given both oral and written instructions about the system. Because there is a high tax imposed on halon, we will investigate switching to newer gases. There is no protection against water damage.

All computer equipment in Zellner 310 is powered by individual or clustered UPS units. Each UPS provides approximately 15 minutes of power during a power interruption.

### **Network Security Safeguards**

All network traffic originating from and destined to the campus passes through a firewall. This firewall is setup with pass and block rules are based on source and destination IP addresses and ports. The firewall is powered by an individual UPS unit, and in the event of a power failure, the firewall is set block all traffic.

### **Types of Computer Service Disruptions**

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve ACU's computing facilities. Additional information that may be needed is provided in the appendices of this document. Supporting documents contain additional hardware, software and vendor information.

#### **Normal computer system problems**

Most of the major hardware and software vendors represented on campus have some kind of remote diagnostic testing for routine problems. Normal response is within four hours for hardware problems. ACU has maintenance contracts for these systems.

Some minor hardware problems do not disrupt service and maintenance is scheduled when convenient for these problems. Most hardware problems disrupting the total operation of the computers are fixed within a few hours.

#### **Major computer and communications system problems**

In most cases, we have test servers that could be used in case of emergency on our primary systems until repairs can be accomplished or the system replaced. Users would be inconvenienced for some amount of time while systems and parameters are adjusted.

#### **Environmental problems (air conditioning, electrical, fire)**

##### *Air Conditioning Outage*

The air conditioning was reconfigured in 2005 to provide a load such that four of the five units will keep the room cool enough in case of failure of a single unit for a short time.

### *Electrical*

In the event of an electrical outage all servers and other critical equipment are protected from damage by Uninterruptible Power Supplies (UPSs). These units will maintain electrical service to our servers long enough for them to be shut down gracefully. Once electrical power is restored the servers will remain "powered down" until the UPSs are recharged a sufficient amount to ensure the servers could be gracefully shut down in the event of a second power failure.

### *Fire*

Zellner Hall Room 310 (the Server Room) is equipped with a halon fire protection system, which will adequately protect the equipment from fires starting in the machine room itself. If a fire starts, the halon system should limit damage to the affected piece of equipment and possibly minor damage to equipment in the immediate vicinity. This would be handled as described in the preceding section: *Major computer and communications system problems*.

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all our hardware.

Humidity factors are not a consideration in the Abilene environment and are not as critical as they once were to computing equipment.

### **Attacks on servers & campus network**

In the event of a disruption of service originating by an attack whether malicious or viral, the first response is to determine the destination of the attack. If the destination is local to the administrative servers, the link to these servers would be disconnected to limit information compromises. If the attack is widespread, then the next step is to determine if the attack originated from within the campus or off-campus. If the attack originated within the campus, this portion of the network would be disconnected. If the attack originated off campus, the Internet connection would be disconnected. The extent of the damage would then be assessed, and the nature of the attack would be investigated so that appropriate preventive measures can be taken before services would be restored.

### **Insurance Considerations**

All major hardware is covered under ACU's standard property and casualty insurance for the University.

## Recovery Teams

In case of a disaster, the team will use the emergency call list. General duties of the disaster recovery coordinator are discussed. Recovery team leaders have been assigned in each major area and general duties given. Assignment of personnel in the major areas to specific tasks during the recovery stage will be made by the team leader over that area.

### **Organization of the Disaster/Recovery Teams**

*Disaster Recovery Coordinator* - Chief Information Officer

#### *Campus-wide Recovery Team*

Chief Information Officer  
Associate Chief Information Officer  
Director, Computing Services  
Manager, Networking Services  
Director, Technology Support Services  
Director, Web Integration & Programming Services  
Director, Adams Center for Teaching & Learning

#### *Academic Systems Recovery Team*

Director, Educational Technology (team leader)  
System Engineers  
System Administrators  
Database Administrators

#### *Administrative Systems/Operations Recovery Team*

Director, Computing Services  
System Engineers  
System Administrators  
Database Administrators  
Programmer/Analysts

#### *Network Communications Recovery Team*

Manager, Networking Services  
Senior Telecom Analyst  
Network Administrator  
Security Administrator  
Telecom Analyst

#### *Campus Communications Team*

Director, Technology Support Services  
Computer Support Analysts  
Team55 staff

### **Disaster/Recovery Team Headquarters**

- If Zellner Hall is usable, the recovery team will meet in Zellner 301.
- If the third floor of Zellner is not usable and other floors are, the team will meet in the Zellner 209.
- If Zellner Hall is hazardous or not usable, the team will meet in the President's Conference Room of the Administration Building.
- If the Administration Building is not usable, the Disaster Recovery Coordinator will be responsible for locating another meeting place on campus.
- If none of the campus facilities are usable, it is presumed that the disaster is of such proportions that recovery of computer support will take a lesser priority. The Disaster Recovery coordinator will make appropriate arrangements.

### **Disaster Recovery Coordinator**

The CIO will serve as Disaster Recovery Coordinator. The major responsibilities include:

- Determining the extent and seriousness of the disaster, notifying the Vice President-Finance immediately and keeping him or her informed of the activities and recovery progress. The Vice President-Finance will in turn keep the President, the Provost and other Vice Presidents informed.
- Invoking the Disaster Recovery Plan.
- Supervising the recovery activities.
- Ensure funding issues are resolved.
- Coordinating with the Vice President-Finance on priorities for clients while going from partial to full recovery.
- Naming replacements, when needed, to fill in for any disabled or absent disaster recovery members. Any members who are out of town and are needed will be notified to return.
- The Director, Technology Support Services will keep clients informed of the recovery activities.

### **Academic Systems Recovery Team Leader Responsibilities**

The Director, Educational Technology will serve as Academic Systems Recovery Team Leader. The responsibilities in this area include recovery in case of complete or partial disruption of services from the central academic systems. Further, with the many academic labs, this group will be responsible for providing services for any disabled academic lab using Technology Support Services and Educational Technology resources.

Responsibilities include:

- Coordinating hardware and software replacement with the academic hardware and software vendors.
- Coordinating the activities of moving backup media and materials from the off-site security files and using these for recovery when needed.
- Keeping the Executive Director, Adams Center for Teaching & Learning, informed of the extent of damage and recovery procedures being implemented.
- Coordinating recovery with client departments, those using the academic computers and/or those using labs.

- Coordinating appropriate computer and communications recovery with the Network Communications Recovery Team Leader.
- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

### **Administrative Systems/Operations Recovery Team Leader Responsibilities**

The Manager, Systems & Operations will serve as Administrative Systems/Operations Recovery Team Leader.

Responsibilities include:

- Coordinating hardware and software replacement with the administrative hardware and software vendors.
- Supervising retrieval of backup media and materials from the off-site storage location and using these for recovery when needed.
- Coordinating recovery with client departments.
- Coordinating appropriate computer and communications recovery with the Network Communications Recovery Team Leader.
- Coordinating recovery of administrative software with client departments.
- Coordinating schedules for administrative programming, production services, and computer job processing.
- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

### **Network Communications Recovery Team Leader Responsibilities**

The Manager, Networking Services will serve as the Network Communications Recovery Leader.

Responsibilities include:

- Coordinating hardware and software replacement with the communications hardware and software vendors.
- Supervising recovery of the computer communications, telephone system and/or cable TV.
- Assigning personnel duties from telecom analysts to project leaders of disaster recovery tasks as needed.
- Coordinating activities of computer and communications recovery with the other Recovery Team Leaders.
- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

### **Campus Communications Team Leader Responsibilities**

The Director, Technology Support Services will serve as the Campus Communications Leader.

Responsibilities include:

- Contact VIP list to begin communication about incident
- Produce regular status reports regarding incident
- Facilitate meetings between team leaders
- Ensure food and other hospitality items are covered for other teams

## Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

### General Procedures

Responsibilities have been given for ensuring each of following actions have been taken and that any updating needed is continued.

- Maintaining and updating the disaster recovery plan. (Associate CIO)
- Ensuring that all ACU technology area personnel are aware of their responsibilities in case of a disaster. (CIO)
- Ensuring that periodic scheduled rotation of backup media is being followed for the off-site storage facilities. (Manager, Systems & Operations)
- Maintaining and periodically updating disaster recovery materials, specifically documentation and systems information, stored in the off-site areas. (Manager, Systems & Operations)
- Maintaining a current status of equipment in the main equipment rooms in Zellner Hall. (Manager, Systems & Operations & Manager, Networking Services)
- Informing all technology personnel of the appropriate emergency and evacuation procedures from Zellner Hall. (Director, Web Integration & Programming)
- Ensuring that all security warning systems and emergency lighting systems are functioning properly and are periodically checked by operations personnel. (Manager, Systems & Operations)
- Ensuring that fire protection systems are functioning properly and that they are checked periodically. (Manager, Systems & Operations & Manager, Networking Services)
- Ensuring that UPS systems are functioning properly and that they are being checked periodically. (Manager, Systems & Operations & Manager, Networking Services)
- Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations. (Director, Technology Support Services)
- Ensuring that the operations procedure manual is kept current. (Manager, Systems & Operations & Manager, Networking Services)
- Ensuring that proper temperatures are maintained in equipment areas. (Manager, Systems & Operations & Manager, Networking Services)

### Backup schemes

- Windows servers
  - We use Symantec's Backup Exec version 11d. It initially performs a full backup on the system. We do daily "synthetic" backup (basically a differential) of the systems and then a weekly full backup. This is not done by doing a full backup on the system in question, but it is created on the backup server by using the last

known full backup and all the daily synthetics since then. This is kept on a 5-week rotation. We keep what is equivalent to a full backup every month for a year. After a year, everything is put back into the pool.

- Unix servers
  - We use Tivoli Storage Manager (TSM) version 5.3.4. It initially performs a full backup on the system as well. But unlike Backup Exec, it only performs differentials every day from that point forward. TSM is able to recreate a full on any given day for as long as we keep the data. The policy is to keep 30 versions of any one file or for no more than 90 days. In other words, if a user changes a file 27 times, but the oldest version is now 91 days old, TSM will delete from tape that 27th file. If only 1 file remains, that file will always be active and not be deleted - the rules that maintain versions only effects files with multiple copies of saved data.
- Desktop computers
  - Daily - This procedure is used to backup all files created or modified each day. This procedure copies files to a network storage device for backup storage. It can be performed at the end of the day or when a client is through using the computer for the day.
  - Weekly - This procedure is used to backup all files. This procedure will also copy all files to a network storage device for backup storage. This procedure needs to be performed on any week day, but should be done consistently once a week on the particular day chosen.

Tivoli's Disaster Recovery Manager (DRM) implemented in summer 2006 allows us to take tapes off site to a bank vault. We make a trip once a week to First Financial Services, downtown Abilene to update the tape repository. This only covers systems backed up by Tivoli.

The backup systems are in Zellner 109, while the servers are in Zeller 310. We are actively looking for another location on campus to further enhance our ability to survive a disaster.

## Recovery Procedures

### Central Facilities Recovery Plan

An incident at the central computing/networking facilities in Zellner Hall may place this plan into action. An incident may be of the magnitude that the facilities are not usable and alternate site plans are required. In this case, the alternate site portions of this plan must be implemented. It is obvious that all major support sections in ACU technology areas will need to function together in a disaster, although a specific plan of action is written for each section.

### Systems & Operations

This portion of the disaster/recovery plan will be set into motion when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode at the central site in a reasonable time.

It is assumed a disaster has occurred and the administrative recovery plan is to be put in effect. This decision will be made by the Vice President - Finance upon advice from the CIO.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
- Notify vendor systems support personnel that help is needed immediately to begin procedures to restore systems software at ACU.
- Order any additional electrical cables needed from suppliers.
- Rush order any supplies, forms, or media that may be needed.

In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternate site:

- Notify officials that an alternate site will be needed for an alternate facility.
- Coordinate moving of equipment and support personnel into the alternate site with appropriate personnel.
- Bring the recovery materials from the off-site storage to the alternate site.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.

- Determine the priorities of the client software that need to be available and load these packages in order. These priorities often are a factor of the time of the month and semester when the disaster occurs.
- Prepare backup materials and return these to the off-site storage area.
- Set up operations in the alternate site.
- Coordinate client activities to ensure the most critical jobs are being supported as needed.
- As production begins, ensure that periodic backup procedures are being followed and materials are being placed in off-site storage periodically.
- Work out plans to ensure all critical support will be phased in.
- Keep administration and clients informed of the status, progress, and problems.
- Coordinate the longer range plans with the administration, the alternate site officials, and staff for time of continuing support and ultimately restoring the Systems & Operations section.

### **Degraded Operations at Central Site**

In this event, it is assumed that an incident has occurred but that degraded operations can be set up at Zellner Hall. In addition to the general steps that are followed in either case, special steps need to be taken.

- Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.
- Replace hardware as needed to restore service to at least a degraded service.
- Perform system installation as needed to restore service. If backup files are needed and are not available from the on-site backup files, they will be transferred from the off-site storage.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the administration and clients informed of the status, progress and problems.

### **Use of Alternate Sites**

If the central site is destroyed, support of critical academic computing activities will be given from the alternate sites. Additional computer systems will be brought in as needed.

Some steps necessary in this process are listed.

- Determine the priorities of client needs and upgrade computers at the academic labs.
- Set up for operations support.
- Coordinate installing additional equipment and moving support personnel.
- When additional, needed equipment is available, move backup materials from the off-site storage area.
- Coordinate restoring any network communications with Networking Services.
- Coordinate client computing support with clients.
- As production begins, ensure that backup procedures are followed and periodic backups are stored off site.
- Work with the Executive Director of the Adams Center for Teaching & Learning, the Provost, and clients in coordinating long-range plans for restoring full support to academic computing resources.

## **Network Communications**

Redundancy is being built into the computer communications systems. We do not have complete redundancy, but most systems have backup equipment and/or cards.

This plan does not, at this time, address the problem of a need for redundancy in the telephone switch system. Considerable funds will be needed for an alternate plan in this area in case of a major disaster in the university telephone switch. Providing adequate air conditioning and fire protection are the highest priority.

Since most of the telephone and computer communications lines are buried and in conduits across campus, connecting lines to alternate sites and to critical areas cannot be done rapidly. For example, it is estimated that if ACU technology areas had to move, it would take 72 hours to restore critical data and voice communications lines.

Some general steps that must be taken in case of a network communications disaster at the central site and/or other parts of the communications network are given.

- Assessment of the damage and an evaluation of steps needed to restore services.
- Assignment of personnel to disaster crews and assignment of tasks. The priority of repairs will be made by the Disaster Coordinator after an evaluation of the critical needs of the University following the disaster.
- If present supplies and equipment on hand are not adequate to restore service as needed, obtain approval for funds needed and contact vendors for priority shipment.
- Coordinate repairs of data communications disasters affecting specific areas of technology support with the recovery team leader of that area.
- Keep the Disaster Recovery Coordinator and team leaders of support areas informed of the extent of the communications damage and recovery procedures being implemented.

A chart of the communications network at ACU is being developed. When it is completed, a copy of this chart will be placed in the off-site storage area and periodically updated.

## **Computer Lab Recovery Plan**

In case of an event affecting only a lab, this section of the disaster plan will be executed. For recovery purposes, labs by definition will mean a computer area supporting a number of clients as contrasted to an area containing only a few microcomputers. An event can occur in an area not defined as a lab; however, it is assumed recovery of services in this situation can be carried out in a routine manner. An area may be considered a lab even if it is in an administrative service area and there are a large number of microcomputers involved.

A disaster will be declared in a lab when a large portion of the units in the lab are affected to the extent that recovery in that area in a reasonable time with normal procedures is not possible.

General steps that will be followed in recovery of a lab are listed. The team leader of the computer area with support duties over the lab affected will assume prime responsibility in the recovery process.

- Determine the extent of the damage in the lab and whether alternate lab services will be needed while recovery is taking place.
- Obtain university approval for any funds needed to replace equipment and supplies.
- Determine whether adequate equipment is available on campus, either from the Campus Store or other areas, to restore even partial services in the lab affected.
- Coordinate recovery of the center with Networking Services if communications lines are involved in the lab.
- If alternate services are to be provided for clients of the lab, coordinate activities between groups affected.
- Keep the Disaster Coordinator informed of the status of the lab and the recovery process.

### **Emergency Procedures**

In case an incident has happened or is imminent that will drastically disrupt operations, the following steps should be taken to reduce the probability of personal injuries and/or limit the extent of the damage, if there is not a risk to employees. Similar steps should be followed, where appropriate, in incidents occurring in a satellite center.

- An announcement should be made to evacuate the building, if appropriate, or move to a safe location in the building. As a preparation for a potential disaster, all ACU technology area personnel should be aware of the exits available.
- If there are injured personnel, ensure their evacuations and call emergency assistance as needed.
- If the computers and air conditioning have not automatically powered down, initiate procedures to orderly shut down systems when possible.
- When possible and if time is available, set up damage-limiting measures.
- Designate available personnel to initiate lockup procedures normal to last shift procedures.

### **Off-site Storage**

All central file backups are made on magnetic tapes or other compact media using an appropriate backup strategy and stored in a room in the lower level of the Brown Library on campus at ACU. Computer & Network Services employees have access to keys both to the exterior doors and to the room where tapes are stored. A copy of the full backups is also stored in a safe deposit box at First National Bank of Abilene, River Oaks branch located at South 14<sup>th</sup> Street and Willis.

### **Other reference documents:**

- Emergency Call List for Information Services
- Full contact information for Information Services and Adams Center for Teaching & Learning employees
- Zellner Hall Emergency Exits Diagram

- Physical Resources Team After Hours & Holiday Emergency Call-Out List
- Server & network equipment inventory
- Primary vendor contact information
- Critical Services Index