

UNIVERSITY OF ARKANSAS PINE BLUFF



DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN TECHNICAL SERVICES

November 2009

DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

TABLE OF CONTENTS

- I. INTRODUCTION**
- II. OBJECTIVES & OVERVIEW**
- III. DISASTER RISKS & PREVENTION**
- IV. DISASTER PREPARATION**
- V. BACKUP PROCEDURES**
- VI. SAFETY ISSUES**
- VII. STRESS AVOIDANCE**
- VIII. DISASTER NOTIFICATION LIST**
- IX. DISASTER RECOVERY TEAM**
- X. ACTIVATING THE DISASTER RECOVERY PLAN**
- XI. EQUIPMENT PROTECTION & SALVAGE**
- XII. DAMAGE ASSESSMENT**
- XIII. EMERGENCY PROCURMENT PROCEDURES**
- XIV. MAINTAINING THE PLAN**

I. INTRODUCTION

This document is the disaster recovery plan for the University of Arkansas at Pine Bluff Technical Services. The information present in this plan guides University management and technical staff in the recovery of computing and network facilities operated by Technical Services in the event that a disaster destroys all or part of the facilities.

A central component to day to day operations at University of Arkansas at Pine Bluff is the consistent availability of IT resources. Any event that interrupts the availability of those resources or the associated data could be referred to as a disaster. Disaster could be as relatively simple as data recovery due to a system failure or as complex as restoration of operations following large scale natural disaster or act of terrorism. Depending on level of disaster, some or all of the following may be required.

The Disaster Recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Technical Services facility at 1200 North University. Each supported computing platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organizational structure for the recovery process.

II. OBJECTIVES & OVERVIEW

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. The University of Arkansas at Pine Bluff certainly is no exception to this trend. Today you can find very powerful computers in every department on campus. These machines are linked together by a sophisticated network that provides communications with other computers across campus and around the world. Vital functions of the University depend on the availability of this network of computers.

Consider for a moment the impact of a disaster that prevents the use of the system to process Student Registration, Payroll, Accounting, or any other vital application for weeks. Students and faculty rely upon our systems for instruction and research purposes, all of which are important to the well-being of the University. It is hard to estimate the damage to the University that such an event might cause. One tornado properly placed could easily cause enough damage to disrupt these and other vital functions of the University. Without adequate planning and preparation to deal with such an event, the University's central computer systems could be unavailable for many weeks.

Primary FOCUS of the Plan

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the University's central computer systems operated by the Technical Services Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

IMPORTANT NOTE!



All disaster recovery plans assume a certain amount of risk, the primary one being how much data is lost in the event of a disaster. Disaster recovery planning is much like the insurance business in many ways. There are compromises between the amount of time, effort, and money spent in the planning and preparation of a disaster and the amount of data loss you can sustain and still remain operational following a disaster.

Time enters the equation, too. Many organizations simply cannot function without the computers they need to stay in business. So their recovery efforts may focus on quick recovery, or even zero down time, by duplicating and maintaining their computer systems in separate facilities.

The techniques for backup and recovery used in this plan do NOT guarantee zero down time. The University administration is willing to assume the risk of data loss and do without computing for a period of time in a disaster situation. To put it in a more economic sense, the University is saving dollars in up-front disaster preparation costs, and then relying upon business interruption and recovery insurance to help restore computer operations after a disaster.

Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup tapes. Significant effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point of the disaster forward.

This plan does not attempt to cover either of these two important aspects of data recovery. Instead, Technical Services recommend that individual users and departments be responsible for a business process establish contingency plans such as collecting paper documents in order to conduct business until technical support is restored, or they may choose to cease operation until technical support is restored.

Primary OBJECTIVES of the Plan

This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to the University of Arkansas at Pine Bluff campus within 14 days of initiation of the plan.
2. Set criteria for making the decision to recover at a cold site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

OVERVIEW of the Plan

This plan uses a "recipe book" approach to recover from a disaster that destroys or severely cripples the computing resources at the Administrative Services Building at 1200 North University in Pine Bluff and possibly at other critical campus facilities.

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan.

Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.



In a disaster it must be remembered that PEOPLE are your most valuable resource. The recovery personnel working to restore the computing systems will likely be working at great personal sacrifice, especially in the early hours and days following the disaster. They may have injuries hampering their physical abilities. The loss or injury of a loved one or coworker may affect their emotional ability. They will have physical needs for food, shelter, and sleep.

The University must take special pains to ensure that the recovery workers are provided with resources to meet their physical and emotional needs. This plan calls for the appointment of a person in the Administrative Support Team whose job will be to secure these resources so they can concentrate on the task at hand.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, magnetic tapes, cds, diskettes, USB drives) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

At the same time, a survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the Cold Site, a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The University will rely upon emergency procurement procedures documented in this plan and approved by the University's purchasing office and the Office of State Purchasing to quickly place orders for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, especially if the plan has not been kept up-to-date. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Restore Data from Backups

Data recovery relies entirely upon the use of backups stored in locations off-site from the Administrative Building. Backups can take the form of magnetic tape, CDROMs, disk drives, and other storage media. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and user data from the backup tapes is done. Individual application owners may need to be involved at this point, so teams are assigned for each major application area to ensure that data is restored properly.

Restore Applications Data

It is at this point that the disaster recovery plans for users and departments (e.g., the application owners) must merge with the completion of the Technical Services plan. Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, the University computer systems can reopen for business. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the Cold Site, physical restoration of the Administrative Building (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the Cold Site are to be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the Cold Site.

III. DISASTER RISKS & PREVENTION

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created.

- Fire
- Flood
- Tornados and High Winds
- Power Outage
- Earthquake
- Computer Crime
- Terroristic Actions and Sabotage

FIRE

The threat of fire in the Administration Building, especially in the computer room area, is very real and poses the highest risk factor of all the causes of disaster mentioned here. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. Not to be forgotten is the hydrogen gas producing batteries in the Uninterruptible Power Supply room where a spark could ignite a fire and explosion. The computers within the facility also pose a quick target for arson from anyone wishing to disrupt University operations.

Preventive Measures

Fire Extinguishers

Hand-held fire extinguishers are required in visible locations throughout the building. Staff is to be trained in the use of fire extinguishers.

Recommendations

Regular review of the procedures should be conducted to insure that they are up to date. Unannounced drills should be conducted by an impartial administrator and a written evaluation should be produced for the department heads housed in the building. Regular inspections of the fire prevention equipment are also mandated. Fire extinguishers are periodically inspected as a standard policy.

FLOOD

Flood waters penetrating the computer room can cause a lot of damage. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections. Of course, the presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel within the computer room.

Preventive Measures

Water detectors should be installed under the computer room floor as well as two sump pumps.

Recommendations

Once the water detectors are installed there should be periodic inspections of the detectors to ensure their proper operation. Batteries within the detectors must be replaced on a regular schedule.

Operators should be trained in shutdown procedures and drills should be conducted on a regular basis. Also, staff in technical services should be trained in responding to victims of electrical shock.

TORNADOS AND HIGH WINDS

The University of Arkansas at Pine Bluff damage due to high winds or an actual tornado is a very real possibility. A tornado has the potential for causing the most destructive disaster we face.

Preventive Measures

While a fire can be as destructive as a tornado, there are very few preventative measures that we can take for tornados. Building construction makes a big difference in the ability of a structure to withstand the forces of high winds. Strong winds are often accompanied by heavy rain, so a double threat of wind and water damage exists if the integrity of the roof is lost.

Recommendations

All occupants of the Administration Building should know where the strong points of the building are and directed to seek shelter in threatening weather. The technical services staff is often unaware of outside weather conditions, so the computer room should be equipped with a weather alert radio. Technical Services should have large tarpaulins or plastic sheeting available in the computer room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage. Operators should be trained how to properly cover the equipment.

EARTHQUAKE

The threat of an earthquake in the Pine Bluff area is low, but should not be ignored. Buildings in our area are not built to earthquake resistant standards like they are in quake prone areas like California. So we could expect light to moderate damage from the predicted quake.

An earthquake has the potential for being the most disruptive for this disaster recovery plan. If the Administration Building is damaged, it is highly probable that the Cold Site on campus may also be similarly affected. Restoration of computing and networking facilities following

a bad earthquake could be very difficult and require an extended period of time due to the need to do wide scale building repairs.

Preventive Measures

The preventative measures for an earthquake can be similar to those of a tornado. Building construction makes all the difference in whether the facility will survive or not. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time. Standby power generators could be purchased or leased to provide power while commercial utilities are restored.

Recommendations

Technical Services should have large tarpaulins or plastic sheeting available in the computer room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage. Operators should be trained how to properly cover the equipment.

POWER OUTAGE

In the event of a power outage all servers and other critical equipment is protected from damage by Uninterruptible Power Supplies (UPSs). These units will maintain electrical services to our servers long enough for them to be shut down gracefully. Once the 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.

Preventive Measures

There should be periodic inspections of the UPSs. Batteries within the UPSs or new UPSs should be replaced or purchased every 3 to 5 years.

Recommendations

In addition to UPSs, also purchase gas generators for long term power outages.

COMPUTER CRIME

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before.

Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. A disgruntled employee can build viruses or time bombs into applications and systems code. A well-intentioned employee can make coding errors that affect data integrity (not considered a crime, of course, unless the employee deliberately sabotaged programs and data).

Preventive Measures

All systems should have security products installed to protect against unauthorized entry. All systems should be protected by passwords, especially those permitting updates to data. All users should be required to change their passwords on a regular basis. All security systems should log invalid attempts to access data, and security administrators should review these logs on a regular basis.

All systems should be backed up on a periodic basis. Those backups should be stored in an area separate from the original data. Physical security of the data storage area for backups must be implemented. Standards should be established on the number of backup cycles to retain and the length of their retention.

Recommendations

Continue to improve security functions on all platforms. Strictly enforce policies and procedures when violations are detected. Regularly let users know the importance of keeping their passwords secret. Let users know how to choose strong passwords that are very difficult to guess. Improve network security. Shared wire media, such as Ethernet, are susceptible to sniffing activities, which unscrupulous users may use to capture passwords. Implement stronger security mechanisms over the network, such as one-time passwords, data encryption, and non-shared wire media.

TERRORISTIC ACTION AND SABOTAGE

The University's computer systems are always potential targets for terroristic actions, such as a bomb. The threat of kidnapping of key personnel also exists.

Preventive Measures

Good physical security is extremely important. However, terroristic actions can often occur regardless of in-building security, and they can be very destructive. A bomb placed next to an exterior wall of the computer room will likely breach the wall and cause damage within the room.

Given the freedom that we enjoy within the United States at this time, almost no one will accept the wide-scale planning, restrictions, and costs that would be necessary to protect the Administration Building from a bomb. Some commonsense measures can help, however.

The building should be adequately lit at night on all sides. All doors into the computer room area should be strong and have good locks. Entrances into the computer room proper should be locked at all times. Only those people with proper security clearances should be permitted into the computer room area. Suspicious parties should be reported to the police (they may not be terrorists, but they may have theft of expensive computer equipment in mind).

Recommendations

Maintain good building physical security. Doors into the computer room area should be locked at all times. All visitors to the computer room should receive prior authorization.

IV. DISASTER PREPARATION

In order to facilitate recovery from a disaster which destroys all or part of the computer room in the Administration Building, certain preparations have been made in advance. This document describes what has been done to lay the way for a quick and orderly restoration of the facilities that Technical Services operates.

The following topics are presented in this document:

- Disaster Recovery Planning
- Recovery Facility
- Replacement Equipment
- Backups
- Disaster Security

Disaster Recovery Planning

The first and most obvious thing to do is to have a plan. The overall plan of which this document is a part is that which Technical Services will use in response to a disaster. The extent to which this plan can be effective, however, depends on disaster recovery plans by other departments and units within the University.

For instance, if the Administration Building were to be involved in the same disaster as Caldwell Hall, the functions of the Controller's Office, or more in particular, the Purchasing Office could be severely affected. Without access to the appropriate procedures, documents, vendor lists, and approval processes, the Computing Services recovery process could be hampered by delays while Purchasing recovers.

Every other business unit within the University should develop a plan on how they will conduct business, both in the event of a disaster in their own building or a disaster at Technical Services that removes their access to data for a period of time. Those business units need means to function while the computers and networks are down, plus they need a plan to synchronize the data that is restored on the central computers with the current state of affairs. For example, if the Payroll Office is able to produce a payroll while the central computers are down, that payroll data will have to be re-entered into the central computers when they return to service. Having a means of tracking all expenditures such as payroll while the central computers are down is extremely important.

Recovery Facility

If a central facility operated by Technical Services is destroyed in a disaster, repair or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at an alternate site.

The University has a number of options for alternate sites, each having a varying degree of up-front costs.

Hot Site

This is probably the most expensive option for being prepared for a disaster, and is typically most appropriate for very large organizations. A separate computer facility, possibly even located in a different city, can be built, complete with computers and other facilities ready to cut in on a moment's notice in the event the primary facility goes offline. The two facilities must be joined by high speed communications lines so that users at the primary campus can continue to access the computers from their offices and classrooms.

Disaster Recovery Company

A number of companies provide disaster recovery services on a subscription basis. For an annual fee (usually quite steep) you have the right to a variety of computer and other recovery services on extremely short notice in the event of a disaster. These services may reside at a centralized hot site or sites that the company operates, but it is necessary for you to pack up your backup tapes and physically relocate personnel to restore operations at the company's site. Some companies have mobile services which move the equipment to your site in specially prepared vans. These vans usually contain all of the necessary computer and networking gear already installed, with motor generators for power, ready to go into service almost immediately after arrival at your site. (**Note:** Most disaster recovery companies that provide these types of subscription services contractually obligate themselves to their customers to not provide the services to any organization who has not subscribed, so looking to one of these companies for assistance after a disaster strikes will likely be a waste of time.)

Disaster Partnerships

Some organizations will team up with others in a partnership with reciprocal agreements to aid each other in the event of a disaster. These agreements can cover simple manpower sharing all the way up to full use of a computer facility. Often, however, since the assisting partner has to continue its day-to-day operations on its systems, the agreements are limited to providing access for a few key, critical applications that the disabled partner must run to stay afloat while its facilities are restored. The primary drawback to these kinds of partnerships is that it takes continual diligence on behalf of both parties to communicate the inevitable changes that occur in computer and network systems so that the critical applications can make the necessary upfront changes to remain operational. Learning that you can't run a payroll, for instance, at your partner's site because they no longer use the same computer hardware or operating system that you need is a bitter pill that no one should swallow.

One of the most critical issues involved in the recovery process is the availability of qualified staff to oversee and carry out the tasks involved. This is often where disaster partnerships can have their greatest benefit. Through cooperative agreement, if one partner loses key personnel in the disaster, the other partner can provide skilled workers to carry out recovery and restoration tasks until the disabled partner can hire replacements for its staff. Of course, to be completely fair to all parties involved, the disabled partner should fully compensate the assisting partners for use of their workers unless there has been prior agreement not to do so.

The use of reciprocal disaster agreements of this nature may work well as a low cost alternative to hiring a disaster recovery company or building a hot site. And they can be used in conjunction with other arrangements, such as the use of a cold recovery site described

below. The primary drawback to these agreements is that they usually have no provision for providing computer and network access for anything other than predefined critical applications. So users will be without facilities for a period of time until systems can be returned to operation.

Cold Site

A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired. There are varying degrees of "coldness", ranging from an unfinished basement all the way to space where the necessary raised flooring, electrical hookups, and cooling capacity have already been installed, just waiting for the computers to arrive.

The University of Arkansas at Pine Bluff has chosen to use the cold site approach for this disaster recovery plan. The necessary agreements are in place for Technical Services to utilize space in one of the other three cores located on campus as its Cold Site. It has adequate space to house the hardware, with some office space available for operating and technical personnel. It has good connectivity to the campus fiber optic network. And a certain amount of preparation has been made for electrical and cooling capacity to support mainframes and network equipment.

Replacement Equipment

This plan contains a complete inventory of the components of each of the computer and network systems and their software that must be restored after a disaster. The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configuration. Where possible, agreements have been made with vendors to supply replacements on an emergency basis. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. The Recovery Management Team will have the expertise and resources to work through these problems as they are recognized. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

Backups

New hardware can be purchased. New buildings can be built. New employees can be hired. But the data that was stored on the old equipment cannot be bought at any price. It must be restored from a copy that was not affected by the disaster. There are a number of options available to us to help ensure that such a copy of your data survives a disaster at the primary facility.

Remote Dual Copy

This option calls for a disk subsystem located at a site away from the primary computer facility and fiber optic cabling coupling the remote disk to the disk subsystem at the primary site. Data written to disk at the primary site are automatically transmitted to the remote site and written to disk there as well. This guarantees that you have the most up-to-the-second updates for the databases at the primary site in case it is destroyed. You can simplify the recovery process by locating the remote disk subsystem at the disaster recovery site. This option is somewhat expensive, but not prohibitively so. It does not require that an entire computer system be built at a hot site, just the disk subsystem. This option is typically limited to mainframe disk systems only.

Automated Off-Site Tape Backup

This option calls for a robotic tape subsystem located at a site away from the primary computer facility and fiber optic cabling (the campus backbone network would be suitable) coupling the subsystem to the primary computer facility. Copies of operating system data, application and user programs, and databases can be transmitted to the remote tape subsystem where it is stored on magnetic tape (optical writable disk media can also be used, but may be more expensive).

While this option does not guarantee the up-to-the-second updates available with the remote dual copy disk option, it does provide means for conveniently taking backups and storing them off-site any time of the day or night. Another huge advantage is that backups can be made from mainframes, file servers, distributed (unix-based) systems and personal computers. Although such a system is expensive, it is not prohibitively so.

Off-Site Tape Backup Storage

This option calls for the transportation of backup tapes made at the primary computer facility to an off-site location. Choice of the location is important. You want to ensure survivability of the backups in a disaster, but you also need quick availability of the backups.

This option has some drawbacks. First, there is a period of exposure from the time that a backup is made to the time it can be physically removed off-site. A disaster striking at the wrong time may result in the loss of all data changes that have occurred from the time of the last off-site backup. There is also the time, expense, and energy of having to transport the tapes. And there is also the risk that tapes can be physical damaged or lost while transporting them.

Some organizations contract with disaster recovery companies to store their backup tapes in hardened storage facilities. These can be in old salt mines or deep within a mountain cavern. While this certainly provides for more secure data storage, considerable expense is undertaken for regular transportation of the data to the storage facility. Quick access to the data can also be an issue if the storage facility is a long distance away from your recovery facility.

The University has opted to taking periodic backups of its primary mainframe systems, databases, file servers, and unix systems and storing those backups in one locations elsewhere on campus. The primary storage location is in Simmons First National Bank, downtown Pine Bluff. The other location is on campus at Com 3 down at Stadium and Administration Building. The tape library at Com 2 is the final storage location where the oldest generation of system and application backup tapes is kept. The actual backup and cycling procedures vary somewhat depending on the computer platform. Details of these procedures are contained in the following document:

Disaster Security

To ensure that an up-to-date copy of this plan is available when a disaster occurs, procedures have been established to store a copy of the plan with other important recovery information at the Cold Site backup tape storage area. Two Lock Boxes should be purchased to hold these materials. The contents of both lock boxes will be identical. One will reside at Simmons First; the other resides in at Com 3 at the Stadium.

When changes to the contents of the lock boxes are necessary, the box at the Com 3 Building is first updated, and then it is taken over to Simmons First and swapped with the box stored there. That box is returned to Com 2 and updated and replaced in Com 3. This ensures that at least one copy of the plan is available at the recovery site. The lock boxes are to remain locked at all times. Keys to the boxes are kept by several key people within the department, including

- Director of Technical Services
- Operations Manager
- Disaster Recovery Plan Coordinator

In a disaster situation when entry into a lock box is needed but the key is not available, you can physically break the lock with bolt cutters.

Transportation and Control of Sensitive Information

In case of the total or partial loss of a facility, the primary processing facility may have to be relocated. In such an event, sensitive information will have to be transported by courier or electronically. The following security measures must be maintained:

An inventory of all files stored in an off-site location must be maintained. A log must be kept of files as they are taken to and retrieved from the off-site location.

Files that are transmitted to a secondary site electronically must be encrypted. A log must be kept indicating when file transmissions occurred and recording the identity of the files transmitted.

Paper files containing confidential information that are transmitted between collection points and a temporary processing facility must be sealed, marked confidential, and a log kept of the

sender and the recipient of the files.

In case of relocation, and if paper and/or magnetic media documents are transported, the log specified in the previous statement of this section will document appropriate user access.

If electronic communications are established, user access control and accountability will be maintained by the user log-on and password system built into the software.

Software and Data Accountability in the Event of Moving to an Alternate Location

If electronic communications are established, software and data will be maintained by the authorized staff. User access control and accountability will be maintained by the user log-on and password system built into the software.

V. BACKUP PROCEDURES

Every system that Technical Services operates is backed up regularly. The backup media for each of these systems is relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes. Three off-site storage locations are used:

- Simmons First National Bank
- Communications Building 3 located at Stadium
- Communications Building 2 located at L.A. Prexy Drive

Four sets of backups exist at any one time. The most recent backups are stored at the Simmons location. The second most recent are stored at the Com 3 location. The third are stored in the tape library at Com 2. And the oldest are stored on an USB drive at the Administration Building.

When a new backup is made, the tapes are rotated through these sites. The new tapes go to Simmons. Its tapes go to Com 3. And its tapes go to Com 2. The tapes at Com 2 are retained for use with the next round of backups.

The procedures for making the backups for each individual computer system differ. In general, media-level or full file system level backups are taken in a given cycle (typically weekly). In some instances, there are additional application-level backups for a system that may be run on a daily basis. Some systems support incremental backups, and these are typically run on a daily basis.

VI. Safety Issues

In almost any disaster situation, hazards and dangers can abound. While survival of the disaster itself can be a harrowing experience, further injury or death following the disaster stemming from carelessness or negligence is senseless.

All personnel must exercise extreme caution to ensure that physical injury or death is avoided while working in and around the disaster site itself. No one is to perform any hazardous tasks without first taking appropriate safety measures.

Hazardous Materials

There are hazardous materials present in the Administration Building. Three primary sources exist for these materials:

- Janitorial supplies - hazardous chemicals are present in the janitorial closets scattered throughout the building. The door to each closet should contain a list of the chemicals present in the closet. If this information is not present at the scene of the disaster, contact the Physical Plant for a list of the chemicals located in the building.
- Battery acid - hazardous battery acid is present in large quantities in the Uninterruptible Power Supply room located in the computer room. Battery acid can cause caustic skin burns, blindness, and pulmonary distress if inhaled. If you come in contact with battery acid, immediately seek a source of water and wash the affected areas continuously until medical assistance can be sought.
- Automotive fluids - hazardous substances related to the operation of a motor vehicle are present in the University Motor Pool garages. These can include, but are not limited to, gasoline, motor oil, brake fluid, antifreeze, lubricants, and battery acid.



Approach any collection of a hazardous material with caution. Notify the nearest safety personnel in the event of a hazardous material spill. Unless you have had the necessary training to do so, do not attempt to clean up a hazardous material spill yourself. Allow the local HAZMAT team to evaluate, neutralize, and clean up any spills.

VII. Stress Avoidance

Recovery from a disaster will be a very stressful time for all personnel involved. Each manager should be careful to monitor the working hours of his staff to avoid over exertion and exhaustion that can occur under these conditions. A good approach is to divide your team members into shifts and rotate on a regular basis. This will keep team members fresh and also provide for needed time with family.

The American Red Cross can also assist with helping to understand the stresses that disaster workers often shoulder.

PTSD - Post-traumatic Stress Disorder is a very real condition that can affect survivors and recovery workers in a disaster. All recovery managers and coordinators should be alert to symptoms in their employees that indicate PTSD and seek assistance from the necessary counseling services. Symptoms usually manifest themselves as:

Intrusions

The individual experiences flashbacks or nightmares where the traumatic event is re-experienced.

Avoidance

The individual tries to reduce exposure to people or things that might bring on their intrusive symptoms.


Hyperarousal

The individual exhibits physiologic signs of increased arousal, such as hyper vigilance or increased startle response.

VIII. DISASTER NOTIFICATION LIST

The disaster notification list for Technical Services is shown below. These people are to be notified as soon as possible when disaster threatens or occurs.

Safety Personnel

	On Campus Dial	Off Campus Dial
Emergency Fire, Ambulance, Rescue, Police, and HAZMAT	8102 or 8103	911
University Police	8102	(870) 575-8102
Physical Plant Main Desk	8831 or 8193	(870) 575-8831

Person	Title	Home Phone	Cellular
Willette Totten	Interim Director of Technical Services	(870) 879-0647	(870) 718-3280
Suwatchara Laohaprasit	Network Administrator		(870) 390-5012
Jacob Jones	Operations Manager		(870) 692-3394
Edward McClusky	Manager of Admin. Computing/Colleague		(870) 718-3332

IX. DISASTER RECOVERY TEAMS

To function in an efficient manner and to allow independent tasks to proceed simultaneously, the recovery process will be handled by teams. This plan calls for eight teams that work together, but for which specific portions of the recovery are assigned.

The eight Disaster Recovery Teams are as follows:

1. Recovery Management Team
2. Damage Assessment Team
3. Facility Recovery Team
4. Network Recovery Team
5. Platform Recovery Team
6. Applications Recovery Team
7. Computer Operations Team
8. Administrative Support Team

The Recovery Management Team oversees the whole recovery process. The other seven teams are represented in the Recovery Management Team. The Recovery Manager leads the Recovery Management Team. The Manager has the final authority on decisions that must be made during the recovery. The Recovery Manager is responsible for appointing the other members of the Recovery Management Team. Each member of the Recovery Management Team will have the responsibility for appointing the other members of the respective team(s).

Selecting Personnel for the Recovery Management Team

The selection of the members of the Recovery Management Team is very important. Since it is almost impossible to document exactly what each of the individual recovery teams will be required to do (each disaster will have its own special set of circumstances, many of which will be completely unanticipated), each member of the Recovery Management Team must be capable of stepping in with the technical and management skills to make the on-the-spot decisions necessary to complete the task at hand.

The discussion that follows identifies those skills that are needed by members of the Recovery Management Team. If these positions are filled with qualified individuals, then the odds for a timely and successful recovery are very high.

Recovery Manager

This individual needs to be a skilled manager/administrator who is accustomed to dealing with pressure situations. He should have a broad knowledge of the hardware and software in use at the site. He should be a "problem solver" as there will be many problems arise that have not been anticipated in advance. He must be able to delegate responsibility to others. He must also have signature authority to expend funds as a part of the disaster recovery process. The current Director of Technical Services is the first choice for the Recovery Manager.

Facilities Coordinator

This individual needs some of the same skills as the Recovery Manager. However, the person also needs to be familiar with the process of getting construction work scheduled and completed on time. The person should be able to understand and oversee the setup of the electrical, environmental, and communications requirements of a data center.

Technical Coordinator

This individual needs to be highly skilled in a number of areas. The person must have a strong background in the setup and interfacing of as many of the platforms in use as possible. The person needs to be able to communicate easily with vendor technical representatives and engineers concerning installation options, performance issues, problem resolution, and a myriad of other things. The person must also be able to schedule and manage people.

Administrative Coordinator

This individual needs to be skilled in the business operations of the University and the State of Arkansas. The person should be well acquainted with the day-to-day operations of a University department. The person should also be a "people person" who can deal with employees and their families during hard times. This person must also be familiar with State purchasing procedures and contracts.

Network Coordinator

This individual needs to be skilled in the area of network design and maintenance. The person should be trained in diagnosing and correcting network outages and in connecting and debugging new additions to an existing network.

Applications Coordinator

First choice for this individual would be someone from the existing application support group. The person should have exposure to a cross section of the currently used applications. The most critical areas are Payroll, Accounting, and Student Records. The person will need to use available tools to ascertain the status of files and data base objects and be prepared to restore later versions from backups if required. The person will also need to interface with users to verify that applications are functioning as expected or analyze and develop solutions to problems that arise.

Computer Operations Coordinator

This individual needs to be skilled in the day-to-day operations of the mainframe systems and software, as well as the knowledge and skills to recreate (or implement new) production schedules for application systems. This person will also be responsible for setting up a limited help desk function that will provide information to callers on status and availability of systems, how to access systems that are in a temporary setting, or any new procedures that users need for submitting their production applications for processing.

Disaster Recovery Team Responsibilities

As the recovery process gets underway, it is imperative that each of the recovery teams remain in close communication and strive to work together to complete the recovery as expediently as possible. The following section provides a brief description of the responsibilities for each team.

Recovery Management Team

The Recovery Management Team is responsible for the coordination of the entire project. It is composed of seven skilled people:

1. Recovery Manager
2. Facilities Coordinator
3. Technical Coordinator
4. Administrative Coordinator
5. Network Coordinator
6. Applications Coordinator
7. Computer Operations Coordinator

The Recovery Manager is the leader of the Recovery Management Team and has the final authority regarding decisions during the recovery process. Each of the remaining individuals will be the leader of a specialized team that will address a portion of the recovery tasks. As the recovery process gets underway, there will likely be areas of overlap between teams and close communication will be required. The Recovery Management Team will have regular meetings scheduled to provide for communication between team coordinators.

Each coordinator should schedule a meeting for members of his team well in advance of their first planned activities. A first-meeting agenda might include:

1. Reviewing the current status of the recovery operation
2. Emphasizing what the team's responsibilities are
3. Making sure that members are aware of any changes to the original recovery plan
4. Assigning tasks to individual team members
5. Setting up time and location for future team meetings

Damage Assessment Team

The Damage Assessment Team will be led by the Technical Coordinator. The person will be responsible for selecting the other team members. Likely choices would be a member(s) from Physical Plant, Operations, and Technical Services. This team will not be responsible for a detailed damage assessment for insurance purposes. The primary thrust for this team is to do two things:

- Provide information for the Recovery Management Team to be able to make the choice of the recovery site.
- Provide an assessment of the salvage ability of major hardware components. Based on this assessment the Recovery Management Team can begin the process of acquiring replacement equipment for the recovery.

Facility Recovery Team

The Facility Recovery Team will be led by the Facilities Coordinator. The person will be responsible for selecting the other team members. Likely choices would be member(s) from Physical Plant, Cold Site Building Representative, and Technical Services.

This team will be responsible for the details of preparing the recovery site to accommodate the hardware, supplies, and personnel necessary for recovery. Detailed layouts and instructions for the Cold Site preparation are included in the recovery plan.

This team will also be responsible for oversight of the activities for the repair and/or rebuilding of the primary site (the Administration Building). It is anticipated that the major responsibility for this will lie within Physical Plant and contractors. However, this team must oversee these operations to ensure that the facility is repaired to properly support the operation of mainframe and networking equipment per the original design of the primary site.

Network Recovery Team

The Network Recovery Team will be led by the Network Coordinator. This person will be responsible for selecting the other team members. Likely choices would be member(s) from Technical Services, End Users, and Physical Plant. It may also be helpful to have the building and/or network manager for the Cold Site building be a part of this team should it be necessary to use the Cold Site.

This team will be responsible for overseeing the restoration of the campus network and all network connections necessary at the recovery site. It is entirely possible in certain disaster situations that the Network Recovery Team may be the only team convened as a result of a campus disaster. For instance, should a fire occur at the Band Building and destroy fiber optic connections and network equipment, this team will be charged with the recovery of operations out of that building or in another building on campus in the most expedient manner.

Because there is such a high degree of reliance on the campus network, for instruction, research, and administrative purposes, very high emphasis must be placed on restoring the network as quickly as possible.

Platform Recovery Team

The Platform Recovery Team will be led by the Technical Coordinator. The person will be responsible for selecting the other members of the team, each of which will be the leader in charge of restoring one or more of the computer platforms described in this plan.

Each team member may recruit others to assist in the technical and detailed work of the recovery. They are responsible for communicating needs and status information to other recovery teams and to coordinate restoration operations between parties working on different computer platforms.

Each platform recovery group will follow this general plan of action:

1. Review damage assessment.
2. Determine which hardware, software, and supplies will be needed to start the restoration of a particular system.
3. Communicate list of components to be purchased and their specifications to the Administrative Support Team.
4. Review the recovery steps documented in this plan and make any changes necessary to fit the situations present at the moment.
5. When hardware begins to arrive, work with vendor representatives to install the equipment.
6. When all components are assembled, begin the steps to restore the operating system(s) and other data from the off-site backup tapes.
7. Attempt to recreate status of all systems up to the point of the disaster if possible. If not, the system is handed off to the Application Recovery Team.

Application Recovery Team

The Application Recovery Team will be led by the Application Coordinator. The person will be responsible for selecting the other team members. This team will be responsible for conducting activities leading up to the approval and acceptance of application systems for production use. In general, this team's activities will begin after the Platform Recovery Team has completed work on the target platform. Some of the team members may in fact be from the platform recovery teams.

Some of the anticipated tasks include:

- Analysis of need for additional recovery activities such as data base restores or individual file restores
- Developing programs/procedures to address specific problems
- Interfacing with application users to test applications

Computer Operations Team

The Computer Operations Team will be led by the Computer Operations Coordinator. This person will be responsible for selecting the other team members. This team will provide three major functions:

1. Man the Help Desk to provide phone assistance and status information to end users.
2. Provide operator staffing for the computer systems at the Cold Site.
3. Provide Production/Control function for establishing production job schedules after systems and applications are restored.

Administrative Support Team

The Administrative Support Team will be led by the Administrative Coordinator. This person will be responsible for selecting the other team members. This team will provide administrative support to the other recovery teams as well as support to employees and their families. One of the most important functions that this team can provide is to take the burden of administrative details so that the engineers and technicians who are responsible for systems recovery can concentrate on their recovery work.

One member of this team should be designated as Family Contact. This person will be available throughout the recovery process to provide assistance to employee family members.

One member of this team should be a designated representative of the University's Purchasing Office. This person will be the liaison to the Controller's Office for the purpose of expediting all emergency purchases and ensuring that proper University and State regulations for purchasing in an emergency are followed. The Purchasing Office has their own Disaster Contingency Plan that they will implement to aid departments needing to restore or rebuild facilities in the event of a disaster.

Some of the anticipated team tasks include:

- ✓ Provide support for executing acquisition paperwork.
- ✓ Assist with the detailed damage assessment and insurance procedures.
- ✓ Determine the status of staff working at the time of the disaster.
- ✓ Provide counseling services for staff or family members having emotional problems resulting from the disaster.
- ✓ Assist the individual Team Coordinators in locating potential team members.
- ✓ Coordinate food and sleeping arrangements of recovery staff as necessary.
- ✓ Provide support to track time and expenses related to the disaster.
- ✓ Provide delivery and transportation services to the Cold Site or other locations as required.
- ✓ Provide public relations support (this function may be provided by University Relations).
- ✓ Assist in contracting with outside parties for work to be done in the recovery process (such as the installation of equipment, or consulting assistance for the installation or recovery of software systems).

X. ACTIVATING THE DISASTER RECOVERY PLAN

Appointment of Recovery Manager

The first order of business is to appoint the Recovery Manager. The person most appropriate for the position is the current Director of Technical Services. If the Director is unavailable, the appointment should be made by the Chancellor. This person must have data center management experience and must have signature authority for the expenditures necessary during the recovery process. You can refer to Disaster Recovery Teams for the responsibilities of the Recovery Manager and a suggested list of people who can fill this and other coordinator roles.

Determine Personnel Status

One of the Recovery Manager's important early duties is to determine the status of personnel working at the time of the disaster. Safety personnel on site after the disaster will affect any rescues or first aid necessary to people caught in the disaster. However, the Recovery Manager should produce a list of the able-bodied people who will be available to aid in the recovery process.

The Recovery Manager should also quickly appoint the Administrative Support Coordinator, whose responsibility it will be to identify anyone injured or killed in the disaster. The Administrative Support Coordinator will work with families and employees, ministering to their needs and obtaining counseling services as necessary.

Taking care of our people is a very important task and should receive the highest priority immediately following the disaster. While we will have a huge technical task of restoring computer and network operations ahead of us, we can't lose sight of the human interests at stake.

Equipment/Media Protection and Salvage

A primary goal of the recovery process is to restore all computer operations without the loss of any data. It is important that the Recovery Manager appoint the Technical Coordinator quickly so that he can immediately set about the task of protecting and salvaging any magnetic media on which data may be stored. This includes any magnetic tapes, optical disks, CD-ROMs, and disk drives. The section Equipment Protection and Salvage contains valuable information on salvaging damaged magnetic media.

Establish the Recovery Control Center

The Recovery Control Center is the location from which the disaster recovery process is coordinated. The Recovery Manager should designate where the Recovery Control Center is to be established. If a location in the Administration Building is not suitable, Simmons First has been designated as the off-site location of the center.

Activating the Disaster Recovery Plan

The Recovery Manager sets the plan into motion. Early steps to take are as follows:

1. The Recovery Manager should retrieve the Disaster Recovery Lock Box located at Simmons First and open it to obtain an up-to-date copy of the Disaster Recovery Plan. This plan is in printed form in the box as well on computer media (diskette or CD-ROM). Copies of the plan should be made and handed out at the first meeting of the Recovery Management Team. The Recovery Manager is responsible for the remaining contents of the Lock Box, which should probably be relocked if possible.

2. The Recovery Manager is to appoint the remaining members of the Recovery Management Team. This should be done in consultation with surviving members of the Technical Services staff and Physical Plant management, and with upper university administration approval. The Recovery Manager's decision about who sits on the Recovery Management Team is final, however.

3. The Recovery Manager is to call a meeting of the Recovery Management Team at the Recovery Control Center or a designated alternate site. The following agenda is suggested for this meeting:

- ✓ Each member of the team is to review the status of their respective areas of responsibility.
- ✓ After this review, the Recovery Manager makes the final decision about where to do the recovery. If Simmons First is to be used, the Recovery Manager is to declare emergency use of the facility and notify President of Simmons or necessary person immediately.
- ✓ The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.
- ✓ Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
- ✓ Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.
- ✓ Each member of the team is to review the makeup of their respective recovery teams. If individual's key to one of the recovery teams is unavailable, the Recovery Manager is to assist in locating others who have the skills and experience necessary, including locating outside help from other area computer centers or vendors.
- ✓ The next meeting of the Recovery Management Team is scheduled. It is suggested that the team meet at least once each day for the first week of the recovery process.

✓

4. The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.

5. An appointed Dean or Vice-Chancellor is responsible for immediately clearing the Recovery Control Center room for occupation by the Recovery Management Team. This includes the immediate relocation of any personnel occupying the room. The Dean or Vice-Chancellor should assist the Administrative Coordinator in locating baseline facilities for the recovery room:

- ✓ Office desks and chairs
- ✓ Telephones
- ✓ Personal computers
- ✓ Hewlett-Packard or Lexmark LaserJet printer
- ✓ Fax machine
- ✓ Copier

6. Mobile communications will be important during the early phases of the recovery process. This need can be satisfied through the use of cellular telephones and/or two-way radios. The Physical Plant and University Police have two-way radio units that may be available upon request.

XI. EQUIPMENT PROTECTION & SALVAGE

This document contains information on procedures to be used immediately following an incident to preserve and protect resources in the area damaged.

Protection

It is extremely important that any equipment, magnetic media, paper stocks, and other items at the damaged primary site be protected from the elements to avoid any further damage. Some of this may be salvageable or repairable and save time in restoring operations.

- Gather all magnetic tape cartridges into a central area and quickly cover with tarpaulins or plastic sheeting to avoid water damage.
- Cover all computer equipment to avoid water damage.
- Cover all undamaged paper stock to avoid water damage.
- Ask the police to post security guards at the primary site to prevent looting or scavenging.

Salvage Magnetic and Optical Media

The magnetic and optical media on which our data is stored is priceless. Although we retain backups of our disk subsystems and primary application systems offsite, magnetic tapes stored in the tape library in the computer room area contain extremely valuable information that would be tough to lose. If the media has been destroyed, such as in a fire, then nothing can be done. However, water and smoke damage can often be reversed, at least good enough to copy the data to undamaged media.

After protecting the media from further damage, recovery should begin almost immediately to avoid further loss. A number of companies exist with which the University can contract for large scale media recovery services.

If more immediate attention is required than can be provided by a contractor, Recovery of Damaged Magnetic Tape and Optical Disk Media describes the recovery process that can be used on-site.

Salvage Equipment

As soon as practical, all salvageable equipment and supplies need to be moved to a secure location. If undamaged, transportation should be arranged through the Recovery Manager to move the equipment to the Cold Site or to another protective area (such as a warehouse) until the Cold Site is ready.



TAKE GREAT CARE WHEN MOVING THE EQUIPMENT TO AVOID DAMAGE.

If the equipment has been damaged, but can be repaired or refurbished, the Cold Site may not be the best location for the equipment, especially if there is water or fire damaged that needs to be repaired. Contractors may recommend an alternate location where equipment can be dried out, repainted, and repaired.

Inventory

As soon as practical a complete inventory of all salvageable equipment must be taken, along with estimates about when the equipment will be ready for use (in the case that repairs or refurbishment is required). This inventory list should be delivered to the Technical Coordinator and Administrative Coordinator who will use it to determine which items from the disaster recovery hardware and supplies lists must be procured to begin building the recovery systems.

XII. DAMAGE ASSESSMENT

This damage assessment is a preliminary one intended to establish the extent of damage to critical hardware and the facility that houses it. The primary goal is to determine where the recovery should take place and what hardware must be ordered immediately.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

In considering the hardware items, consider first the equipment lists provided in the recovery sections for each platform. These lists were constructed primarily for recovery at the cold site so they consist of the critical components necessary to recovery. You will need to separate items into two groups. One group will be composed of items that are missing or destroyed. The second will be those that are considered salvageable. These "salvageable" items will have to be evaluated by hardware engineers and repaired as necessary. Based on input from this process, the Recovery Management team can begin the process of acquiring replacements.

With respect to the facility, evaluation of damage to the structure, electrical system, air conditioning, and building network should be conducted. If estimates from this process indicate that recovery at the original site will require more than 14 days, migration to the cold site is recommended.

XIII. EMERGENCY PROCUREMENT PROCEDURES

The success or failure of this plan's ability to ensure a successful and timely recovery of the central computer and network facilities hinges on our ability to purchase goods and services with lightening speed.

The Arkansas State Purchasing Regulations lend themselves to a very liberal interpretation which provides the University with considerable latitude in emergency procurement of goods and services. The University's Purchasing Office should have a disaster recovery plan of their own that will assist departments in the rapid turnaround of emergency procurements.

The liberal policy for emergency procurement, coupled with extensive Business Interruption Insurance, provides the Recovery Manager with a sound basis for aggressive recovery actions. Perhaps now is the time for a word of caution. There will always be a day of reckoning following every exciting event, when those actions taken under the stress of the moment will be examined and evaluated in the light of normality. You can significantly reduce your anxiety level in the eve of such an accounting by following preset rules and directives - to the extent possible under the circumstances - and most importantly, keeping records and logs of transactions.

The Administrative Support Coordinator is responsible for all emergency procurement for Computing Services. All Disaster Recovery Team members must submit their requests to the Coordinator. The Coordinator will follow the regulations established for emergency procurement and will work with the Buyer that has been appointed by the Purchasing Office to complete the acquisition. If the Purchasing Office has been so severely affected by the disaster that it cannot function, the Coordinator is directed to work with the Office of State Purchasing in Little Rock for all emergency procurements.

(In this latter case, the University should use every means possible to convince the Office of State Purchasing to send their representative to Pine Bluff to handle purchasing transactions on-site in the fastest manner possible.)

The Administrative Support Coordinator is also responsible for tracking all acquisitions to ensure that financial records of the disaster recovery process are maintained and that all acquisition procedures will pass audit review.

The Administrative Support Coordinator must also be aware of the University's insurance coverage to know what is and is not allowed under our policies. In the event an item to be purchased is disallowed by insurance coverage, or if expenses exceed the dollar limits of the insurance coverage, the Coordinator must consult with the Recovery Manager and other responsible University personnel (such as the University's Finance Administrator).

XIV. MAINTAINING THE PLAN

Having a disaster recovery plan is critical. But the plan will rapidly become obsolete if a workable procedure for maintaining the plan is not also developed and implemented. This document provides information about the document itself, standards used in its construction, and maintenance procedures necessary to keep it up to date.

Web Server Accessible

This disaster recovery plan has been designed to be accessible as a World Wide Web document retrievable from a web server. This makes it easy to access the plan for periodic review and provides a convenient means for structuring the plan in an online fashion.

This plan will be made available through the University's World Wide Web server (<http://www.uapb.edu>) in order to make it more generally available to University staff. But more importantly, a web document format permits it to be published in an online form that can be stored on CD-ROM or USB flash drive media for viewing with the most popular Internet Browser. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Online publishing makes these changes immediately available to all those who are interested.

Test & Evaluation

The plan will be routinely evaluated once each year. All portions of the plan will be reviewed by Technical Services. In addition the plan will be tested on a regular basis and any faults will be corrected. The Disaster Recovery Plan coordinator has the responsibility of overseeing the individual documents and files and ensuring that they meet standards and consistent with the rest of the plan.

A combination of the following action will be accomplished annually.

1. Structured Walk-Through Testing

During a structured walk-through test, disaster recovery team members meet to verbally walk through the specific steps of each component of the disaster recovery process as documented in the disaster recovery plan. The purpose of the structured walk-through test is to confirm the effectiveness of the plan and to identify gaps, bottlenecks or other weaknesses in the plan.

2. Checklist Testing

A checklist test determines if sufficient supplies are stored at the backup site, telephone number listings are current, quantities of forms are adequate, and a copy of the recovery plan and necessary operational manuals are available. Under this testing technique, the recovery team reviews the plan and identifies key components that should be current and available. The checklist test ensures that the organization complies with the requirements of the

disaster recovery plan. A combination of the checklist test and the structured walk-through test is suggested for initial testing to determine modifications to the plan before attempting more extensive testing.

Change-Driven Maintenance

It is inevitable in the changing environment of the computer industry that this disaster recovery plan will become outdated and unusable unless someone keeps it up to date.

Changes that will likely affect the plan fall into several categories:

1. Hardware changes
2. Software changes
3. Facility changes
4. Procedural changes
5. Personnel changes

As changes occur in any of the areas mentioned above, Technical Services management will determine if changes to the plan are necessary. This decision will require that the managers be familiar with the plan in some detail. A document referencing common changes that will require plan maintenance will be made available and updated when required.

Changes that affect the platform recovery portions of the plan will be made by the staff in the affected area. After the changes have been made, Technical Services will be advised that the updated documents are available. They will incorporate the changes into the body of the plan and distribute as required.

Changes Requiring Plan Maintenance

The following lists some of the types of changes that may require revisions to the disaster recovery plan. Any change that can potentially affect whether the plan can be used to successfully restore the operations of the department's computer and network systems should be reflected in the plan.

Hardware

- ✓ Additions, deletions, or upgrades to hardware platforms.

Software

- ✓ Additions, deletions, or upgrades to system software.
- ✓ Changes to system configuration.
- ✓ Changes to applications software affected by the plan.

Facilities

- ✓ Changes that affect the availability/usability of the Cold Site location.
- ✓ Changes to Administration Building that affects Cold Site choice such as enlargement cooling or electrical requirements etc.

Personnel

- ✓ Changes to personnel identified by name in the plan.
- ✓ Changes to organizational structure of the department.

Procedural

- ✓ Changes to off-site backup procedures, locations, etc.
- ✓ Changes to application backups.
- ✓ Changes to vendor lists maintained for acquisition and support purposes.