University of Arkansas at Little Rock

Business Continuity Plan

August 30, 2003

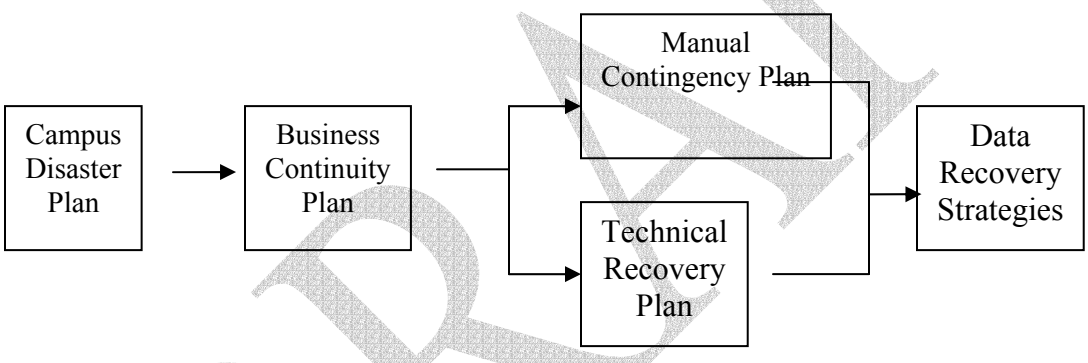
Draft

Table of Contents

Section 1: Plan Overview

Introduction
The Business Continuity Plan (BCP) for the University of Arkansas at Little Rock (UALR) integrates business risk management, operational risk management, and business continuity. The plan recognizes a tiered approach to ensure the university is managed during a disaster that renders the technical infrastructure inoperable for a period exceeding two days. There are three important steps in managing the university during and after a disaster occurs. The first step will be implemented by activating the Campus Disaster Plan which ensures that health, life and safety issues are addressed prior to the activation of this plan. The BCP includes a two-tiered approach to managing and restoring functionality after a disaster with three primary goals:

1. Facilitate continued performance of essential business functions of the university until the technical infrastructure can be restored.
2. Activate the technical recovery plan that will be used to restore the technical infrastructure to full functionality.
3. Implement data recovery strategies to update the Banner system to ensure it remains up to date.



This plan was developed by a cross-functional team to address the needs of the university in the event of a crises (2-5 days) or a disaster (over 5 days) that renders the campus network and computer systems infrastructure inoperable.

Business Continuity Development Team
Amy Barnes, Communications
Mike Beaird, Law School Library
Larry Dickerson, College of Education
Charles Ford, College of Information Services and Systems Engineering
Jim Golden, College of Professional Studies
Dennis Fleming, Computing Services
Sam Howell, Student Services
Lynette Jack, Ottenheimer Library
Jim Menth, College of Information Services and Systems Engineering
Diane Newton, Finance
Cindy Milazzo, Administration
Jerry Stevenson, Provost
Jeannie Winston, CIO, Chair

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

Scope and Limitations
The Business Continuity Plan will be executed after health, life and safety issues are addressed. Health, life and safety issues are addressed in the Campus Disaster Plan that is administered by the Associate Vice Chancellor of Administration.

Objectives
- The development and testing of a well-structured and coherent plan which will enable UALR to recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts normal business operations by rendering the technical infrastructure inoperable for a period exceeding two days.
- Establish cohesive emergency response and crisis management plan.
- Develop a communications plan to notify teams, activate the plan, assemble personnel, assess damages, and declare a disaster.
- Define mission critical processes using a Business Impact Analysis.
- Define manual processes that can be implemented until the technical infrastructure is restored.
- Develop a plan to recover and restore the technical infrastructure to the UALR campus.
- Establish criteria for making the decision to recover at a cold site or repair the affected site.
- Describe an organizational structure for implementing the plan.
- Provide information concerning the types of personnel who will be required to implement the plan and define the skills and knowledge required.
- Identify the equipment, floor plan, procedures, and other items necessary for the technical recovery.
- Communicate the plan to the campus community.

Assumptions
- Health, life and safety issues are addressed by the Campus Disaster Plan
- The library collection is not in imminent danger of loss
- Restoration of utilities is addressed in the Campus Disaster Plan
- This plan covers catastrophic events. Planned and unplanned downtime of less than two days are not addressed.
- The Business Impact Analysis drives IT Restoration and Recovery Strategies.
- Prevention is the most important aspect of continuity planning.
- The Recovery Point Objective (RPO) defines the amount of data that can potentially be lost in the event of a disaster. The RPO for the Banner system is six (6) days.
- The Recovery Time Objective (RTO) is the time frame in which the technical infrastructure is to be restored. The RTO is not quantified due to the lack of a redundant data center and the unknown variables of how long it will take to prepare a cold site in the event that FH is damaged beyond use.
- This plan will be reviewed and updated annually.

Recommendations

- Conduct media relations training for senior management who may be required to interface with the media during a disaster
- Install a generator in FH and move air conditioning compressors to a more protected location (feasibility study is $6,500)
- Seal the windows in FH (estimated cost of $33,000)
- Move critical servers in FH to a location that is less susceptible to water leak from wet labs in the floors above the data center

Section 2: Mission Critical Processes and Systems

Mission critical processes and systems are identified on the following Business Impact Analysis matrix. This matrix was developed by the BCP Team and is based on the impact to the campus community. While the impact may vary depending on the timing of an event, the matrix assumes the university is in normal operating mode when the event occurs.

Business Impact Analysis Matrix

Infrastructure	Crisis			Disaster		
	High	Medium	Low	High	Medium	Low
Power/Utilities (1)	X			X		
Network	X			X		
Banner	X			X		
• Payroll						
• Registration						
• Records						
• Financial Aid						
• Purchasing						
• Accounts Payable						
• Accounts Receivables						
• Bookstore						
• Health Services						
• Card Access System						
• Admissions						
E-mail		X		X		
Web Server			X		X	
Phones (2)			X			X
Image Now			X		X	

Function	Crisis (2-5 Days)			Disaster (Over 5 Days)		
	High	Medium	Low	High	Medium	Low
Communications	X			X		
Research Labs	X					X
Library (3) (4)		X				X
Teaching on-line courses (4)			X	X		
Teaching web enhanced courses			X			X

Assumptions:

1. Utilities are a function of the campus disaster plan.
2. Phones can be restored parallel to other activities.
3. The library collection is intact with no danger of massive losses.
4. Teaching on-line courses and the library are parallel activities that are performed by different groups.

Section 3: Risk Analysis

A threat is an event that causes a disruption in the normal university operating environment of more than two days. UALR recognizes two major types of threats: human and environmental/natural.

Human threats include:
Sabotage
Terrorism
Virus
Bomb threats
Robbery/thefts
Hackers

Environmental and natural threats include:
Tornado – physical damage
Loss of power
HVAC
Flood
Fire – FH or ADS high risk, others moderate
Ice and/or snowstorm
Lighting
Wind damage
Earthquake

Based on the above types of threats, the BCP team developed the following Risk Assessment Matrix to identify what types of risk are high. The risks that are defined as high have contingency plans developed to address prevention and controls to mitigate risks.

Risk Assessment Matrix

Human Risk	High	Moderate	Low
Virus	X		
Hackers/Crackers	X		
Loss or absence of key personnel on crisis teams	X		
Sabotage		X	
Bomb Threat			X
Terrorism			X

Environmental Risk	High	Moderate	Low
Loss of power	X		
Ice/snow	X		
Flood	X		
Water leak in critical areas	X		

Fire (FH or ADS)		X	
HVAC		X	
Tornado (physical damage)			X
Lightning			X
Wind damage			X
Earthquake			X

Add timeline for decision points
Add conditional perspective for each threat.

Improve physical security.

Based on the Risk Assessment Matrix, UALR recognizes the following type of threats as high risk for our campus.

- Virus
- Hackers/Crackers
- Loss of technical personnel
- Loss of power to FH
- Ice/Snow
- Flood
- Water leak in critical areas in FH

Disaster Risks and Prevention

It is important to take reasonable measures to prevent a disaster or to mitigate the potential of one. 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 human and environmental/natural.

COMPUTER CRIME (include viruses and hackers/crackers)

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 have the latest virus protection software. UALR has a site license for McAfee and it is available at no charge to individual users.

All systems should have the latest patches applied to operating systems. Computers without the latest patches are more vulnerable to attack and can have a devastating impact on the campus network.

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 thinnet 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.

Loss of technical personnel

The technical recovery plan addresses the loss of technical personnel.

Loss of power to FH

The best method of ensuring the University is protected against a loss power is to purchase and install a generator in FH 213.

Ice/Snow

The most likely result of an ice or snow storm is the loss of power associated with damage to the commercial electric utility facilities that provide power to the UALR campus. The best method of dealing with the potential damage of ice or snow is to follow the same course of action for loss of power and purchase and install a generator in FH 213.

FLOOD (includes water leak from wet lab on floors above the data center)

The Fribourgh Hall Building is located on an area of elevation and is surrounded by lower ground. The Computing Services Data Center is on the second floor of Fribourgh Hall is not likely to flood from natural causes, however internal flooding from a broken pipe is a real threat. Not only could there be potential disruption of power caused by the water, a broken pipe can cause damage to cable plant or other sensitive electrical connections. Additionally, the presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel within the machine room.

Preventive Measures

Machines should not be located under pipes from the floor above. Care should be taken to move existing machines to areas of the machine room that are not under water pipes. Water detectors should be installed under the raised floor and should be tested regularly.

Recommendations

Periodic inspections of the under flooring in the machine room must be conducted to detect water seepage.

Install an environmental monitoring system in FH 213 that will alert specified technical personnel if water is detected in the room. Periodic inspections of the water detectors are also required 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 the machine room should be trained in responding to victims of electrical shock.

Additional threats to FH 213

Additional threats to the technical infrastructure include fire, tornados and high winds, earthquake, and hazardous materials in FH. Even though these threats are not rated as high risk, each one is addressed individually due to the potential for extensive damage should one or more occur.

FIRE

Fribrough Hall is filled with electrical devices and connections that could overheat or short out and cause a fire. Additionally, there are hydrogen gases 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. Wide area fires, such as those common in recent years in California, are also a possibility in dry times.

Preventive Measures

Fire Alarms

The Fribourgh Hall Building is equipped with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building.

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.

Building Construction

The Fribourgh Hall Building is built primarily of non-combustible materials. The risk to fire can be reduced when new construction is done, or when office furnishings are purchased, to acquire flame resistant products.

Training and Documentation

Detailed instructions for dealing with fire are present in Standard Operating Procedures documentation. Staff are required to undergo training on proper actions to take in the event of a fire. Staff are required to demonstrate proficiency in periodic, unscheduled fire drills.

Recommendations

Regular review of the procedures should be conducted to ensure 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.

A Halon fire suppression system should be installed in the data center. Equipment should be wired to be shut down with the press of a button located near the entrance/exit of the data center.

Smoke detectors located under the machine room raised flooring should be periodically inspected and cleaned.

TORNADOS AND HIGH WINDS

Although tornados and high winds are rated as low risk, the potential damage caused by a tornado on the campus could severely damage or destroy Fribrough Hall. In the event that Fribrough Hall is destroyed, the likelihood of being able to rebuild the technical infrastructure in a timely manner is greatly diminished.

Preventive Measures

Building construction makes a big difference in the ability of a structure to withstand the forces of high winds. Fortunately, Fribourgh Hall Building is a strong building. The exterior walls are solid concrete. The data center has small movable windows; however the handles are removed to keep the windows closed. 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 Fribrough Hall should know where the strong points of the building are and directed to seek shelter in threatening weather. The machine room operator is often unaware of outside weather conditions, so the machine room should be equipped with a weather alert radio.

Computing Services should have large tarpaulins or plastic sheeting available in the machine 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 Little Rock area is low, but should not be ignored. Scientists have predicted that a large earthquake along the New Madrid fault may happen any time in the next 50 years, and that its effects will be felt as far away as our area. 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 Fribourgh Hall 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 for 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

Computing Services should have large tarpaulins or plastic sheeting available in the machine 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 proper cover the equipment.

Hazardous Materials

The risk of hazardous material was not rated nor discussed by the BCP. It is mentioned because of the presence of such items in Fribrough Hall and the possibility of consequences if the building is damaged by a tornado, high winds or an earthquake.

There are hazardous materials present in the Fribourgh Hall Building. Four primary sources exist for these materials:

1. Janitorial supplies - hazardous chemicals are present in the janitorial closets scattered throughout the building. The door to each closet contains 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.

2. Battery acid - hazardous battery acid is present in large quantities in the Uninterruptible Power Supply room located in the extreme northwest corner of the first floor of the building. 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.
3. Hazardous Material Storage Area is just outside the entrance to Fribourgh Hall Building and is storing unknown hazardous material.
4. The Floors above the Data Center house Chemistry and Biology Labs. Either of which can have toxic biological or chemical hazards.

Section 4: Roles and Responsibilities

Emergency Response Teams

Roles and responsibilities are defined utilizing a similar tiered approach based on the same structure as activating the Campus Disaster followed by the Business Continuity Plan. The initial assessment is performed under the scope of the Campus Disaster Plan. The next phase is to activate the Business Continuity Plan and assemble the Crisis Management Team. The third phase is to concentrate simultaneously on executing manual processes and restoring the technical infrastructure. The final phase is to recover any data that has been lost due to the disaster. The roles and responsibilities in each phase are included in this section.

Initial Assessment Team

As stated in the introduction, UALR utilizes a tiered approach to disaster planning and recovery. The Initial Assessment Team (IAT) will execute the first tier Campus Disaster Plan for the Departments of Public Safety and Physical Plan. Members of the IAT are first responders in the event of a crisis or disaster. The IAT will be activated by the Associate Vice Chancellor of Facilities.

The responsibilities of the IAT include understanding the scope of the situation, coordinating physical and safety recovery efforts, and monitoring the situation. The Associate Vice Chancellor for Facilities, as a member of the IAT, will be responsible for notifying the CMT of the status of an event. The Chancellor, as a member of the IAT, will be responsible for designating a disaster and activating the BCP.

Business Continuity Crisis Management Team (CMT)

Once the IAT has ensured that the campus is a safe working environment and that life, health and safety issues are addressed, the Business Continuity Crisis Management Team (CMT) is activated by the Chancellor. The CMT will be responsible for managing the business recovery and resumption efforts and will communicate with both internal and external campus constituencies. The CMT will report to the Emergency Operations Center (EOC). The primary site for the EOC is designated as the Chancellor's Conference Room on the third floor in Administration South. The secondary site for the EOC is designated as the first floor of Dickinson Hall. In the event both the primary and secondary site are not accessible, the CMT will meet in the Don W. Reynolds Center.

The CMT is composed of the Chancellor, Vice Chancellors, and the CIO. Refer to Appendix A for contact information.

Technical Recovery Management

After the CMT has reported to the designed EOC and assessed the damage, the technical recovery will be managed by Computing Services. The Technical Recovery Management Team will be composed of the CIO and Associate Directors of Computing Services. Refer to Appendix B for contact information.

Data Recovery Management

When the technical recovery is completed to a point where the Banner system is restored to full functionality, the individual users will be responsible for entering any data that was lost due to

the disaster and any data that was manually processed during the disaster. Both the technical and data recovery responsibilities are defined in the following roles and responsibilities matrix.

Roles and Responsibilities Matrix

This matrix was developed by the BCP Team based on the mission critical systems and processes in the BIA matrix that is located in Section 2 of this plan.

Role or Function	Responsible	Accountable
Power/Utilities	Director, Physical Plant (Dave Millay)	AVC Facilities (Cindy Milazzo)Lucian Shockey
Network	AD Networks (Rogers Davis)	CIO (Jeannie Winston)
Banner	AD MIS Banner User's Group (Tracy Johnson)	CIO (Jeannie Winston)
• Payroll	Manager, Payroll (Dorothea Yates Linda Johnson)	AVC Finance (Diane Newton)
• Registration	Manager, Registration (Sandra Dannaway)	Division Chief (Sam Howell)
• Records	Manager, Records (Sandra Dannaway)	Division Chief (Sam Howell)
• Financial Aid	Manager, Financial Aid (John Noah)	Division Chief (Sam Howell)
• Purchasing	Manager, Purchasing (Mike Shepherd)	AVC Finance (Diane Newton)
• Accounts Payable	Manager, Accounts Payable (Dorothea Yates Bruce Anderson)	AVC Finance (Diane Newton)
• Accounts Receivables	Manager, Accounts Receivables (Dorothea Yates Gina Fielder)	AVC Finance (Diane Newton)
• Bookstore Vouchers	Bookstore Manager (Brenda Thomas)	Division Chief (Preston Slayden)
• Card Access System	AD MIS (Tracy Johnson) (Rogers Davis)	CIO (Jeannie Winston)
• Admissions	Manager, Admissions (John Noah)	Division Chief (Sam Howell)
• Admissions (Law School)	Manager????	????
E-mail	AD Networks (Rogers Davis)	CIO (Jeannie Winston)

Web Server	Project Specialist (CS) (Pat Pearce)	AD Networks (Rogers Davis)
Phones (2)	AD Networks (Rogers Davis)	CIO (Jeannie Winston)
Image Now	Manager, Records (Sandra Dannaway)	Division Chief (Sam Howell)
Communications	Director (Amy Barnes)	VC Advancement (Bill Walker)
Research Labs	Individual Academic Departments	Provost (David Belcher)
Library (3) (4)	Library MIS (Lynette Jack)	Director, Library (Kathy Sanders)
Teaching on-line courses (4)	OCCP (Sonja Sanderson)	AVC Provost (Linda Musun)
Teaching web enhanced courses	StaR (Aimee Dixon)	AVC Provost (Linda Musun)
Electronic Course Delivery		
○ WebCT	StaR (Aimee Dixon)	AVC (Linda Musun)
○ Comppressed Video	StaR (Aimee Dixon)	AVC (Linda Musun)
○ Streaming Video	Star (Aimee Dixon)	AVC (Linda Musun)

A flowchart of the emergency Roles and Responsibilities is included in Appendix C.

Section 4.A: Communications Plan

This plan is available through the University's World Wide Web server 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 diskette or CD-ROM media for viewing with a Netscape browser in file browse mode. 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.

Communication to the campus and external communities during a disaster will be sent via e-mail after the e-mail system is restored.

Other ideas include setting up a voice line with recorded messages updated regularly.

All media requests will be addressed by the Office of Communications or the Crisis Management Team.

Do we need to consider communication with UA System, BOT, BOV?

Could also make pocket cards for all employees or for key employees.

Section 6: Contingency Plans and Restoration

Contingency Plans

Both Student Services and Financial Services will maintain contingency plans defining how they will conduct manual processing until limited network and system functionality can be restored. The one exception to the departmental plan is the contingency plan for payroll that is included in this plan. After a disaster is declared, the Bank of America will be notified to continue paying the last payroll until the Banner system has been restored and a new payroll can be generated.

This payroll contingency plan has two time frames when it is will not be sufficient to meet the payroll needs for the campus. These two time frames coincide with the beginning and ending of the academic calendar. Personnel Action Forms specifying the employment periods for nine-month faculty begin in mid-August and end in mid-May. If the disaster occurs immediately before the fall semester, new and returning faculty will need manual paychecks. If the disaster occurs immediately after the last payroll for faculty at the end of the spring semester, nine-month faculty will be paid when they are not due a paycheck.

The following list of UALR employees are authorized to notify the Bank of America that UALR is declaring a disaster.

Chancellor	Dr. Joel Anderson
Vice Chancellor for Finance and Administration	Lucian Shockey

Anyone else???

The Bank of America requests ____ days advance notice that a disaster has been declared and requests the notification be submitted in writing to _____?????

The Memorandum of Agreement with the Bank of America and the procedures by which it can be executed is located in Appendix D.

The list of essential functions and personnel for Finance and Administration and Student Services is included in Appendices E and F, respectively.

Restoration and Recovery Strategies

Based on the functions identified in the BIA, systems will be restored in the following order in either a crisis or disaster:

1. Campus network (in part at the backup location or in whole depending on the situation)
2. Banner
3. E-mail
4. Web Server
5. WebCT

Desktop personal computers should be distributed to Computing Services, Student Services and Financial Services. A minimum of ten should be distributed to each department.

Technical Recovery Management

The technical recovery is the responsibility of Computing Services. A technical recovery plan that restores systems in the above order is under development and will be located in SUB 205 and FH 213.

Data Recovery Management

Each department will be responsible for entering data into the Banner system that has been manually processed during a disaster.

Emergency Procurement Procedures

The Arkansas State Purchasing Regulations provides considerable latitude in emergency procurement of goods and services.

The Technical Recovery Management Team will be responsible for all emergency procurement for Computing Services. All purchases must follow the regulations established for emergency procurement and will work with the UALR Purchasing Office to complete the acquisition. If the Purchasing Office has been so severely affected by the disaster that it cannot function, a member of the Technical Recovery Management Team will work with the Office of State Purchasing in Little Rock for all emergency procurements. If this is necessary, the Office of State Purchasing will be requested to send a representative to campus to handle purchasing transactions on-site in the most efficient manner possible.

The Technical Recovery Management Team is 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.

Arkansas State Purchasing Regulations are included in this plan in Appendix G.

Once a disaster has been declared and equipment purchasing needs have been identified, the state outlines emergency requisition procedures. These procedures are included as Appendix H.

Section 6: Campus Awareness

Educational Awareness Materials

Place educational awareness materials here.

Ideas include:

Laminate brightly colored stock paper with simple, basic procedures.

Distribute to all employees.

Include in employee orientation.

Glossary of terms included in Appendix I.

Appendices

Appendix A	Continuity Management Team Contact Information
Appendix B	Technical Recovery Team Contact Information
Appendix C	Flowchart of Roles and Responsibilities
Appendix D	Memorandum of Agreement with the Bank of America
Appendix E	Essential Functions and Personnel for Finance and Administration
Appendix F	Essential Functions and Personnel for Student Services
Appendix G	Arkansas State Purchasing Regulations
Appendix H	Purchasing Procedures and Forms
Appendix I	Glossary

Appendix A

Continuity Management Team Contact Information

Position	E-mail address	Work Phone	Home Phone	Cell Phone or Pager Number
Chancellor Joel Anderson	jeanderson@ualr.edu	(501) 569-3200		
Vice Chancellor for Academic Affairs and Provost David Belcher	dobelcher@ualr.edu	(501) 569-3204		
Vice Chancellor for Student Services Charles Donaldson	**cwdonaldson@ualr.edu**	(501) 569-3328		
Vice Chancellor for Financial Services Lucian Shockey	**lxshockey@ualr.edu**	(501) 569-3202		
Vice Chancellor for University Relations Bill Walker	**wxwalker@ualr.edu**	(501) 569-3186		
Chief Information Officer Jeannie Winston	**eewinston@ualr.edu**	(501) 569-3344	(501) 227-8443	(501) 837-8466

Appendix B

Technical Recovery Management Team Contact Information

Position	E-mail address	Work Phone	Home Phone	Cell Phone or Pager Number
Chief Information Officer Jeannie Winston	eewinston@ualr.edu	(501) 569-3344	(501) 227-8443	(501) 837-8466
Associate Director Networks Rogers Davis	redavis1@ualr.edu	(501) 569-8719		(501) 960-4415
Associate Director MIS Tracy Johnson	tljohnson@ualr.edu	(501) 569-8413		(501)
Associate Director Administration Dennis Fleming	dbfleming@ualr.edu	(501) 569-8709		(501)
Associate Director Desktop Support Julio Fuentes	exfuentes@ualr.edu	(501) 569-8413		

Appendix C

Flowchart of Emergency Roles and Responsibilities

Appendix D

Memorandum of Agreement With the Bank of America (For Payroll)

Lucian Shockey will prepare the information for this section

Appendix E

Essential Functions
For
Finance and Administration

Appendix F

Essential Functions
For
Student Services

Appendix G

Arkansas State Purchasing Regulations

ARKANSAS STATE PURCHASING REGULATIONS: The appropriate regulations are quoted below.

"19-11-233. Emergency procurements.

The State Purchasing Director, the head of a purchasing agency, or a designee of either officer may make or authorize others to make emergency procurements as defined in _ 19-11-204(9) and in accordance with regulations promulgated by the director.

R1:10-11-233. Emergency Procurements.

(A) Bids. The State agency must, at a minimum, receive three (3) competitive bids unless the emergency is critical. The quotation abstract must show the names of at least three (3) firms contacted in attempting to obtain competition.

(B) Approval. All emergency procurements shall be approved in advance by the State Purchasing Director, the head of a purchasing agency, or a designee of either officer. Where time or circumstance does not permit prior approval, approval must be obtained at the earliest practical date. Requests for approval shall be made in writing and shall include:

(1) a copy of the purchase order;

(2) a copy of the quotation abstract; and

(3) a written explanation of the emergency.

(C) Reports. Reports, which may include a copy of the purchase order, quotation abstract and explanation for the previous month on emergency procurements, shall be submitted by each Agency Purchasing Official to the State Purchasing Director no later than the tenth of the month following the reporting period.

(D) Tie Bids. In the event the lowest prices offered result in a tie bid, the person responsible for awarding a contract must insure that (1) all offers meet specifications and (2) Arkansas Preference does determine award. After the above-listed determinations are made, an award will be made by lot (flip of a coin). The coin flip will be done by the person responsible for awarding the contract in the presence of a witness. The witness must be an employee of the State of Arkansas. A documentation of the coin flip must be included on the tabulation or bid history sheet and be signed by both parties."

Appendix H

Purchasing Procedures and Forms

EMERGENCY REQUISITION PROCEDURES:
Obtain a Requisition number from Computing Services Requisition number list.
Fill-in Quotation Abstract Item Description Page with descriptions of items and/or services for which quotations are being solicited (e.g., equipment make and model numbers, installation services for equipment/software listed, etc.)
Quotation Abstract

Item Description Page

Unit Extended Hardware/Software Description Quantity Price Price
---

Enter description of equipment here

Shipping and Handling charges, FOB Little Rock, Arkansas _____

TOTAL: _____

Delivery Time: _____ days.
FAX the Item Description Page to at least three vendors likely to be able to provide needed goods or services. Call the vendor to insure that they know the FAX has been sent and understand the need for a quick response. Timeframes for responses can be very short; just be reasonable for the goods requested.

Summarize the vendor responses to the Quotation Abstracts on the Quotation Abstract, Quotation Summary Page.

Quotation Abstract
Quotation Summary Page

Requisition Number: _____
Date: _____

Person Requesting: _____
Phone: _____

Bidders contacted: (at least three; attach additional abstracts if necessary)
Company Name: _____
Address: _____
_____
_____
_____
Contact: _____

Phone: _____
FAX: _____
Quote: _____

Company Name: _____
Address: _____
_____
_____
_____
Contact: _____
Phone: _____
FAX: _____
Quote: _____

Company Name: _____
Address: _____
_____
_____
_____
Contact: _____
Phone: _____
FAX: _____
Quote: _____

Attach the vendor responses, any contacts or agreements, and the Quotation Summary Page to Requisition(s) made out for the lowest qualified bids.

If quotations are completed during normal University business hours, provide the Requisition, Quotation Abstracts, and any contracts to the Purchasing Office for issuance of Purchase Orders. Due to the immediate need, Purchase Order numbers should to be called to the appropriate vendor or copies should be Faxed, depending upon the policies of the vendor(s) receiving the order(s).

If the quotations are completed after hours, instruct the appropriate vendors to proceed with processing the order. Obtain the purchasing approvals and Purchase Orders as soon as possible during the next available business hours.

If no University purchasing staff are available due to the nature of the disaster, instruct the appropriate vendors to proceed with processing the order, and forward Requisition(s) and Quotation Abstract(s) to the Office of State Purchasing for issuance of Purchase Order(s).

Appendix H
Glossary

Disaster – any event which disables or interrupts the ability to maintain a business as usual environment for a period of time that adversely affects the mission of the university.

High availability – systems that are available 24/7 without down time for maintenance.

RPO – recovery point objective – the point in time in which data can be recovered after a disaster.

RTO – recovery time objective – the time frame it takes to recover a system.

HAZARD OR THREAT IDENTIFICATION: The process of identifying situations or conditions that have the potential to cause injury to people, damage to property, or damage to the environment.

HUMAN THREATS: Possible disruptions in operations resulting from human actions. (i.e., disgruntled employee, terrorism, blackmail, job actions, riots, etc.)

Environmental and natural threats: Events caused by nature that have the potential to impact an organization.