



IT Disaster Recovery and Business Continuity Plan

Health Sciences Building.....11.....
Kinkead Annex Building.....11.....
Math-Science Building.....11.....
Plant Operations Building.....11.....

Introduction

The purpose of this disaster recovery plan is to identify the business processes of the University of Arkansas Fort Smith that are dependent upon information technology and outline the recovery procedure.

Scope

The information technology services to be addressed in this plan are all components of hardware, software, networks, and telecommunications located on the campus of the University of Arkansas - Smith.

Users/organizations affected

The Information Technology Services Department at the University of Arkansas Fort Smith provides information technology resources and support for both the administrative and academic needs of the University. The Information Technology Services Department is the service organization responsible for the proper functioning of the Data Center, servers, networks, desktop computers, and telephone systems. All production information technology resources reside on the main campus in 2 different 5.9 (S3 (m))-3.4 (p)

Should a disaster occur which causes this disaster recovery team to convene, the Vice Chancellor of Finance and Administration should notify the Director of Information Technology Services if the disaster has any possibility of causing disruption to the information technology systems or the telephone system (i.e., tornado, fire, flood, earthquake, etc.).

Date of Plan

Updated August 2011

Updated November 2011

Updated July 2012

Updated December 2012

Updated August 2016

Updated January 2017

Updated August 2018

Updated January 2019

Updated August 2019

Updated February 2019

Updated October 2020

Updated July 2021

Updated July 2022

Notification to Media and Employees

The Director of Marketing and Communications is responsible for handling news media contacts to campus and issuing statements or releases from campus. He is also responsible for sending alerts to employees. UAFS uses the Lions Alert system by Rave Alerts as the method of notification for employees during a disaster. The Rave Alert system is hosted on campus by Rave. Employee contact information for email, cell phone and landline phone is stored in this system. The Chief of University Police Department has administrative access to send alerts.

Critical applications/services that must be restored:

Order of Importance

Unitrends Backup – Unitrends backup is on a appliance on campus and is copied to a Unitrends appliance at UAMS in Little Rock, AR

Recovery Team Leader: Mike Ming, Manager of IT Infrastructure

Team Member: Rick Creekmore, Windows Admin

Internet Connectivity - AREON

NOC

Phone—877-398-0012 (toll free)
Phone- 317-274-0223
Website— noc.aron.net
Recovery Team Leader: Mike Ming- Manager of IT Infrastructure
Team Member: Jason Scott- Network Engineer
Team Member: Lorne Tippit- IT Technician

Networking equipment

Recovery Team Leader: Mike Ming- Manager of IT Infrastructure
Team Member: Jason Scott- Network Engineer
Team Member: Lorne Tippit- IT Technician

Banner –Alpha1.uafortsmith.edu AIX Server [physical server] Banner Forms Server slbanformsp01

Recovery Team Leader: Pam Fout- Associate Director;
Team Members: Mike Ming- Manager of IT Infrastructure, Network Admin; Veronica Frederick – Database Admin, Rick Creekmore- Server Admin and Hayden Woodhull- Server Admin
Domain Controllers – need to be restored while Barracuda data is restored.

Recovery Team Leader: Mike Ming- Manager of IT Infrastructure

Team Member: Rick Creekmore- Server Admin, Hayden Woodhull- Server Admin

1. Schema Master and Infrastructure Master Domain Controller for ad.uafortsmith (dc03.ad.uafortsmith.edu physical server) and PDC Emulator, Domain Naming Master, and RID Master (dc01.ad.uafortsmith.edu physical server)
2. Domain Controller for student.ad.uafortsmith.edu (stu01.student.ad.uafortsmith.edu physical server)

VMware Environment – Dell Blade Chassis, Dell Blade servers, Dell EqualLogic storage, Dell Compellent storage, and Dell switches

Recovery Team Leader: Mike Ming- Manager of IT Infrastructure

Team Member: Hayden Woodhull

Team Member: Rick Creekmore

Team Member: Jason Scott

Blackboard Learn – (SaaS) Should only be affected by domain controllers to grant login access

Recovery Team Leader: Mike Ming- Manager of IT Infrastructure

Team Member: Hayden Woodhull- Server Admin

Team Member: Pam Fout- Associate Director

Telephone

Recovery Team Leader: Natalie Rie- Telephony Admin

Team Member: Lorne Tippit- IT Technician

SQL Server (SQLsrv01.ad.uafortsmith.edu virtual server)

Recovery Team Leader: Rick Creekmore- Systems Admin

Team Member: Mike Ming- Manager of IT Infrastructure, Terry Meadows - IT Director

Vcenter server for VMWare (SWVcenterP01 physical server)

10. Copy of the BDMS software (Ellucian)
11. Copy of the Banner Workflow software (Ellucian)
12. All virtual servers are on the Unitrends backup system
13. All physical servers can be restored as virtual servers

Data File Backups:

1. Banner Oracle DB backup file
2. Blackboard Transact Oracle DB backup file
3. Main website DB backup file (MySQL)
4. Evisions DB backup file (Access database)

Backup retention periods

Keep current backups for a period of 14 days

Secure off-site storage and backup locations and procedures

Vital Records Control - VRC Companies LLC (was Central Records)

www.vitalrecordscontrol.com

301 Rogers Avenue 72901

Fort Smith, AR

479-782-7779

Customer ID 8278

- 1] Lyndsey St John (main contact) Director of Operations - Fort Smith
After hours (Lyndsey St John 479-459-2591) (Manuel Flores 479-806-0558)
- 2] Call one of the phone numbers and let them know we are coming on site
- 3] Go on site to Vital Records (see address above)
- 4] Show ID to verify you as being on the University of Arkansas at Fort Smith approved list
- 5] Users on the approved list: Cheryl Davis, Mike Ming, Pam Fout, Rick Creekmore, Terry Meadows, Veronica Frederick, Hayden Woodhull
- 6] Passcode: BLUE CUP

Acquisition and replacement hardware

Should it be needed minimum system requirements if hardware replacement is necessary.

Alternative processing site

DR Location

UAMS Data Center

4401 W. 7th

Little Rock, AR 72205

SOC Support Line (Call for any and all needs)

501-686-5793

Alternative meeting site (must be over 3 miles from campus)

The Bakery District

Disaster Recovery Plan Test Procedure / T-06174-392.0 (s) 00190.3396.97813 State

(Beta1)), backup home server, redundant domain controller, backup

2. Switch to virtual processing via the replicated Dell Compellent Storage and racked ESXi servers in the Gardner Server room.
3. Place emergency orders to Dell Computer Systems for personal computers for labs
4. Place an emergency order to Dell Computer Systems for Blade Chassis, Blade servers, rack servers, Compellent storage, and Dell switches to connect everything
5. Place emergency orders to CISCO Systems for Ethernet network switches
6. Restore services using the order of importance
7. Restore servers and applications from tape or Unitrends appliances

Sebastian Commons and Lion's Den

The Sebastian Commons buildings are residential apartments and the Lion's Den buildings are residential dorms. Should the following buildings be lost:

1. Work with Campus Services to identify temporary location for staff offices and student housing
2. Place emergency orders to Dell Computer Systems for personal computers
3. Place emergency orders to CISCO Systems for Ethernet network switches
4. Restore services using the order of importance

Boreham Library

Breedlove Building

Business Center Building

Campus Center Building

Echols Building

Flanders/BII Building

Fullerton Building

Old Gymnasium Building

Health Sciences Building

Kinthead Annex Building

Math- Science Building

Plant Operations Building

Recreation and Wellness Center Building (RAWC)

Stubblefield Center

Vines Building

51st Annex Police Building

Windgate Building

If any of these buildings are lost:

1. Work with Campus Services to identify temporary location for faculty and staff offices, classrooms, and labs
2. Place emergency orders to Dell Computer Systems for personal computers

3. Place emergency orders to CISCO Systems for Ethernet network switches
4. Restore services using the order of importance

Sign Off

This page is to be signed and dated each time the disaster recovery plan is reviewed.

Updating the plan

The following actions should be accomplished annually