UAFS

UNIVERSITY OF ARKANSAS - FORT SMITH

IT Disaster Recovery and Business Continuity Plan

Table of Contents

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 - Fort 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 data centers in Fort Smith, Arkansas. The University leases half a server rack at UAMS that is currently housing the Unitrends DR backup appliance.

Responsible parties for initiating the plan

Disruptions in computer and telephone services can arise from many causes. It is important that disruptions be identified as early as possible and proper notification is made so steps can be taken to minimize the damage and/or start the recovery process as quickly as possible. In this way, the disruption of service and its negative impact on the activities of the University can be minimized. The disaster recovery team is listed below.

Pam Fout
Work: 479-788-7452
Cell: 479-650-4042

Terry Meadows
Work: 479-788-7891
Cell: 479-459-5187

Mike Ming
Work: 479-788-7474
Cell: 479-235-8511

Vice Chancellor of Finance
Carey Tucker
Work: 479-788-7035
Cell: 318-658-3114

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 Dec 2012
Updated Aug 2016
Updated Jan 2017
Updated Aug 2018
Updated Jan 2019
Updated Aug 2019
Updated Feb 2019
Updated Oct 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 send 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 off-campus by Rave. Employee contact information for email, cell phone and landline phone is stored in this system. The Chief of the 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 an 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 - Call Here for Support
      Email – noc@areon.net

Phone – 877-398-0012 (toll free)
Phone - 317-274-0223
Website – noc.areon.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 (stu-dc01.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 Rice – Telephony Admin
Team Members: Lorne Tippit – IT Technician

SQL Server (SQLsrv01.ad.uafortsmith.edu virtual server)
Recovery Team Leader: Rick Creekmore – Systems Admin
Team Members: Mike Ming - Manager of IT Infrastructure, Terry Meadows – IT Director

Vcenter server for VMWare (SWVcenterP01 - physical server) –

Recovery Team Leader: Mike Ming - Manager of IT Infrastructure
Team Member: Rick Creekmore - Server Admin

Blackboard Transact – Door access and LionsCash (BBtsDB.ad.uafortsmith.edu – virtual transact database server, BBtsuafs.ad.uafortsmith.edu – virtual transact front end server)
Recovery Team Leader: Mike Ming - Manager of IT Infrastructure
Team Member: Rick Creekmore - Server Admin

Uafs.edu – Online web site is in the cloud
Recovery Team Leader: Chris Kelly – Director of Marketing and Communications

Evisions – Maps Server includes Intellicheck, FormFusion, Argos (swevisionp01.ad.uafortsmith.edu virtual server)
Recovery Team Leader: Mike Ming - Manager of IT Infrastructure
Team Member: Rick Creekmore - Server Admin, Michael Madzar – Security Analyst

ID Card machine and SP75+ ID Card printer
Recovery Team Leader: Darren Smith – Senior PC Systems Analyst;
Team Member: Blake Frost – Manager

BDMS (bdms01.ad.uafortsmith.edu virtual server)
Recovery Team Leader: Mike Ming - Manager of IT Infrastructure
Team Member: Rick Creekmore - Server Admin

Banner Workflow (bworkflow-prod virtual server)
Recovery Team Leader: Mike Ming - Manager of IT Infrastructure
Team Member: Rick Creekmore - Server Admin

Pharos – printing (pharos.ad.uafortsmith.edu physical server)
Recovery Team Leader: Rick Creekmore, Windows Server Admin
Team Member: Blake Frost – Project Manager

Service Now (SaaS)
Recovery Team Leader: Jo Ann Parker – IT Specialist
Team Member: Pam Fout – Associate Director

Software and data file backups needed to restore critical applications.

The software needed to restore critical applications are:
1. Copy of the current production source of Banner software (Ellucian)
2. Copy of the Oracle Forms Server software (Oracle)
3. Copy of the Oracle Database Server software (Oracle)
4. Copy of multiple versions of Microsoft SQL Server (Microsoft)
5. Copy of Microsoft Server 2019 (Microsoft)
6. Copy of Microsoft Server 2016(Microsoft)
7. Copy of Microsoft Server 2012 (Microsoft)
8. Copy of the latest release of the Blackboard Transact software (Blackboard)
9. Copy of the Evisions Maps, Argos, Intellicheck, FormFusion software

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 phones 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 Procedures

Monitoring

The following actions should be reviewed annually

1. Review critical applications to ensure they are current
2. Review of alternate storage/operating requirements and procedures
3. Review of roles and responsibilities

Test and Evaluation

The following actions should be tested during the year

1. Multiple recoveries of files, directories, or full servers
2. Two table top DR simulations or real life actual disaster recoveries such as a server or data center outage

Deficiencies identified during the testing process should be used to make improvements and modification to the plan as necessary

Recovery Documentation

Basic DR documentation can be found on the main web site uafs.edu, which is hosted offsite by Databank. All other documentation can be found on the UAFS Home Server which is backed up on our Unitrends appliance and it replicated to a secondary home server located in another data center.

Alternative procedures for users

So that users can cope with the unavailability of the computer application during the recovery period (these documented manual procedures should be included as part of the DRP).

Recovery of facilities

Gardner Building

The Gardner Building houses the primary Data Center for the UA Fort Smith campus (GB-205). GB-205 contains the primary server equipment (IBM P7) for ERP Banner system, the campus home server, domain controller, and backup virtual environment. A backup ERP Banner server (IBM P7 alternate

(Beta1)), backup home server, redundant domain controller, and backup virtual server environment are housed in the Data Center of the Baldor Building. These servers are continuously operating. The production database archive logs are copied from the IBM P7 Alpha at 15-minutes intervals to the IBM P7 alternate server (Beta1). Should the entire Gardner Building be lost or the equipment in GB-205 destroyed due to localized damage to that area of the building, the P7 alternate (Beta1) with its associated forms server located in the Baldor Building would provide operational support for Banner services with the potential loss of no more than 15 minutes of on-line transactions. (The database would be restored from backup and the production archive logs would be applied.)

It is noted that should both the Gardner Building and the Baldor Building be lost due to a massive tornado, earthquake, or disaster of enough scale to level a sizeable area, both facilities might be lost. To cover this possibility, we are planning on moving Banner SIS to the Oracle cloud with a "lift and shift".

The Gardner Building houses the main campus network and the campus telephone system (including the telephone demarcation point). Telephone data communications is split between 2 buildings. One PRI is in Gardner and one PRI is in Baldor.

Should the telephone room on the second floor of the Gardner Building be lost:

1. Notify CISCO Systems and place an emergency order for a main campus switch and building Ethernet network switch
2. Notify AT&T to recover the telephone demarcation facility
3. Plan an emergency order for a campus telephone switch
4. Work with Campus Services to identify temporary location for faculty and staff offices, classrooms, and labs
5. Restore services using the order of importance

Should the Gardner Building be lost:

1. Switch to P7 alternate (Beta)
2. Limit the number of on-line users to 50
3. Notify users of potential loss of up to 15 minutes of transactions
4. Use personal computers from undamaged buildings for temporary servers using the order of importance
5. Load the servers from backup tapes from the offsite storage location if necessary (Central Records), the swNASP01 server located in Baldor, or from the Unitrends backup appliances located on site or at UAMS in Little Rock
6. Place emergency order to IBM Corporation or 3rd party vendor for P Series server or equivalent
7. Place emergency orders to Dell Computer Corporation for PC-Servers
8. Place emergency order to CISCO Systems for replacement of building Ethernet switches

Baldor Building

The Baldor Building contains a secondary Data Center for servers including the main VMware virtual server environment. Should the Baldor Building be lost?

1. Work with Campus Services to identify temporary location for faculty and staff offices, classrooms, and labs

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
Kinkead 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

1. Plan updated to reflect all additions, changes, or deletions as a result of plan monitoring.
2. Plan updated to reflect all additions, changes, or deletions as a result of plan test and evaluation.
3. Date of finalization of plan update.

Terry Meadows
Director of Technology   Date: 7/22/2022
/s/ Terry Meadows