DISASTER RECOVERY PLAN

For

UNIVERSITY COMPUTING

Fayetteville State University

21 May 2002

PREFACE

This document titled Disaster recovery plan is simply a plan that addresses immediate and temporary restoration of computing and network operations after a natural or manmade disaster within defined timeframes. Business continuity plan, on the other hand, is the ability to maintain continued availability of processes and information across the enterprise during and beyond the post-recovery period. We did not address the later issue of making continued availability of technology and information as their scope depends on the extent of the damage on campus. However, due to the well established system back-up procedures in place, we will not loose any information or data stored on those systems in the event of a disaster. We have identified the mission critical systems, an alternate site, hardware and staff to operate the mission critical system, and client connectivity mechanisms to the critical systems for a period of six months. Our assumption is that we will be able to plan and orchestrate a true business continuity plan during those six months.

This document, like any business plan, is a living document. As such, the Director of Information Technology Services will keep this document updated as our environment changes.

Arasu T. Ganesan
CIO and Associate Vice Chancellor for Information Technology
Fayetteville State University, NC

FAYETTEVILLE STATE UNIVERSITY

COMPUTING AND NETWORK DISASTER RECOVERY PLAN

Purpose

To resume Information Technology Systems Operations within five to one hundred eighty days after a "disaster" has occurred at Fayetteville State University.

Objectives

This document provides the general information that is required to reestablish the Fayetteville State University's Administrative Computing Center and the associated operational environment when a local disaster occurs.

Scenarios

1. Total loss of the Information Technology Services Center and all network Main Distribution Frames (MDFs). The on-site recovery storage area's contents are destroyed. This event would require complete restoration of the Data Center and all Network MDFs. This event would require re-installation of software systems and data files that were stored at the off-site facility. The replacement of unusable hardware equipment - including enterprise computers, network cables, hubs, switches, terminal servers, terminals, printers, and networked computers is required. Widespread restoration of power supply for the computing and networking utilities would be the norm.

2. Partial loss of the Information Technology Services Center and network Main Distribution Frames (MDFs). The on-site disaster recovery storage vault and contents remain intact. This event would also require complete restoration of the Data Center and all Network MDFs. This event would require re-installation of all non-recoverable software systems, using the contents of the disaster recover vault, and repair or replacement of unusable hardware equipment - including enterprise computers, network cables, hubs, switches, terminal servers, terminals, printers and networked computers. Minor restoration of power supply for the computing and networking utilities would be required.

3. Partial loss of components of the Information Technology Systems Center and critical network Main Distribution Frames (MDFs). Selected aspects of scenarios one or two would be applied based on the extent of partial loss. It is unlikely that the total extent of partial loss could be absolutely categorized immediately, but the computing and networking capabilities could be restored incrementally using a planned pattern of recovery.

Assumptions

The design of the Disaster Recovery Plan is based on the following assumptions:

1. Emergency resources (budget, personnel, and materials) and staff can be made available.

2. End users will implement pre-planned manual operations while the Information Technology Services department (Administrative Computing and Networking -- i.e., Telephone Systems and Data Communications) are out-of-service, and will retain transactional data to be entered into the data bases of the restored Information Technology Systems Center when the system becomes available.

3. FSU designated staff will have immediate access to all contingency plans for the computing and networking infrastructure and related contingency plans from strategic functional areas: Chancellor's Office, Business and Financial Affairs, Student Affairs (Housing), Registrar and Admissions.

4. FSU Management, coordinated through the Chancellor's senior staff, will procure qualified personnel, equipment, materials and other resources as needed.

5. The site for temporarily restoring the Information Technology Services Center will be the Health Physical Education Building where sufficient space will be available. The likely site for temporarily restoring the Networking Main Distribution Frames will be in the Health Physical Education Building. If the Health Physical Education Building is not available, due to the nature of the disaster, another site must be determined.

6. Disaster recovery software and backup databases and files will survive the disaster in either the on-site or the off-site facility and they will be accessible.

7. Replacement computing, telephone and data communications equipment will be available from vendors within seven to sixty days depending on the capabilities of vendors to meet FSU's response requirements.

8. It may not be feasible to restore to the Information Technology Services Center and Telecommunications configurations (e.g., exact capabilities) pre-event status; Users may be required to make adjustments to computing resources access channels and to the characteristic of jobs that must be run in the newly restored computing configuration(s).

9. In the case where the disaster completely destroyed the FSU Administrative Computing Center (Butler Building), the back-up site will be used to run critical jobs until new hardware can be acquired and installed.

Events Include

Natural disasters:

- Catastrophic collision
- Earthquake
- Explosion
- Fire
- Flood
- Hurricane/tornado
- Mechanical failure(s)
- Electrical power malfunctions

Induced:

- Carelessness
- Criminal Activities
- Disgruntled Employee(s)
- Ignorance
- Mentally disturbed person(s)
- Malicious mischief
- Terrorism
- Internet/Intranet intruder attacks

Resources Affected

1. Air Conditioning
2. Communications Equipment
3. Data Bases
4. Data Cartridges/Tapes
5. Documentation
6. Electric Power
7. Facilities
8. Hardware: Computing and Peripheral
9. Master Files
10. Personnel
11. Systems and Applications Software

Disaster Recovery Teams

Four teams will carry out the Disaster Recovery Plan (s):

1. Management
2. Damage Assessment
3. Recovery Team
4. Technical

Management

If a "disaster" occurs that disables FSU's computing and networking services, the Management Team will be responsible for the disaster recovery process. The group must establish an adequate information processing and networking environment to support fundamental business and student support activities. Functional areas that have local information processing operations will be responsible for their disaster recovery paradigm(s).

The Management Team will be responsible for making decisions and determining directions based on information received from the Damage Assessment Team.

The Management Team will interface with all constituents to inform them of status of the disaster and direct recovery activities. The Special Assistant to the Chancellor will chair the Management Team. The Chancellor will be kept up-to-date on the extent of the damages and the recovery process. The Recovery Team for review and approval of the Management Team will develop a recovery schedule. The Recovery Team will then execute the plan.

Damage Assessment

The process for determining the extent of the disaster and what is required to reestablish the computing and networking services is as follows:

1. The operations staff that is on duty will notify the Manager of Information Technology Systems and the Special Assistant to the Chancellor that a disaster has occurred which disabled the computing and networking services. If no operations personnel is on duty, the campus police will notify the Special Assistant to the Chancellor who will in turn notify the Assistant Director of Information Technology Systems so she can assemble the Damage Assessment Team. The Special Assistant will also notified the Chancellor and alert the Management Team. If the building or the wing that houses the computer center is completely destroyed, the recovery team will be assembled immediately. The facilities management staff and capital projects people will develop the plan for restoring the building. The initial action will be to determine if the storage vault is in- tact. Efforts will be undertaken to provide access to the vault just in case some of the contents are needed for the recovery of the computing center.

2. The Director of the Information Technology Systems will assemble the Disaster Assessment Team. This team will determine the severity of the disaster by collecting the following information as outlined below. If the building or wing was destroyed, the Director of Information Technology Systems will assemble the Recovery Team instead of the Damage Assessment Team.

Damage Assessment Team.

- If operations staff were on duty, the status of personnel will be determined. Immediate notification will be given to Special Assistant for appropriate actions.
- Preliminary assessment of what is required to become operational
- To what extent essential resources were damaged?
- Is the on-site storage vault assessable?
- Is an alternate site required?

The Damage Assessment Team will determine the status of each administrative system, especially the Financial Records (FRS) and Student Information System (SIS). If access to the computer room is denied due to the extent of damages, this team will terminate all efforts and the Recovery and the Management Teams will be notified.

Recovery

The Recovery Team will have access to the Disaster Recovery Plan and other relevant materials and information processing resources that will be needed to restore the computing center and the campus-wide networking infrastructure to a base-line functional capability. The team will also review the inventory of program listings, FSU developed application documentation, operating systems manuals, hardware and computer systems manuals to ensure completeness. If application reference manuals are need, they will be requested from the application software provided. The team will be responsible for obtaining all relevant documentation from the secured off-site disaster recovery storage, if required, and subsequently ensure their delivery to the new/temporary computer or network equipment rooms. The materials that were removed from the storage site will be replaced as soon as copies can be made. This team will be responsible for reestablishing the University's computing and networking capability.

The Disaster Recovery Plan will be reviewed with the end users to assure that the critical tasks are clearly defined and that the procedure(s) for accomplishing those tasks are understood. Based on this process of clarifications, the end user will be asked to establish appropriate temporary business environments to carry out essential academic and administrative activities. These temporary business environments may exist for thirty to sixty days, depending on progress of disaster recovery efforts. If it appears that the recovery will take more than 14 days, a backup site will be negotiated for processing key application transactions. The exact recovery process will be determined once the Damage Assessment has determined how extensive the damage was to the Computing Center. However, the capability exist for full recovery in the event that we had total destruction of the computer center with no more than one day of lost transactions. Backups of the data are taken daily and monthly.

The monthly backup is a stand alone back up of the operating system. The daily backups that are taken includes the applications and all of the data. These backups are taken at the end of the production cycle. In addition to these daily backups, at the beginning and end of the production cycle for each application, a backup of the data is taken. While this is somewhat redundant, our intent is to reduce the amount of data that must be reentered into the system if a disaster occurs. The backup tapes can be used to restore the system to current status. The users may be required to reenter only one day of pre-disaster transactions. When significant changes are made to the operating systems, the monthly standalone will be taken. A copy of all documentation that is pertinent to the recovery, operation and management of the computing center as well as the backup tapes can be retrieved from either vault.

The Information Technology Systems production control personnel, telecommunications (campus telephone systems and data communications) and facilities management personnel will staff this group. Members will supervise vendor activities in restoring emergency computing and networking capacities. The Recovery Team will be chaired by the Director of Information Technology Systems.

<u>Technical</u>

The Technical Team will determine the state of transactional processing available on the appropriate backup volumes stored in the off-site storage vault. The team will assist the end user in collecting unprocessed transactions and assist in data preparation or input operations.

Once a disaster occurs, the end users will do manual processing and keep an accurate account of all transactions. When the system has been made operational, the FRS, HRS and SIS users must coordinate and synchronize their efforts to enter transactions into the system that occurred while the system was not operational. Once the first day's manual transaction have been entered and the daily batch processing has occurred, the next day's transactions will be entered and the process will be repeated until all transaction have been entered and processed. Daily and weekly batch processing will be done as appropriate to allow the processing of all transactions that had been done manually. When this effort has been completed the system will be made available for normal processing.

The Information Technology Systems Administrative Applications Analysts and key SIS, HRS and FRS end users will staff this group. There will be an FRS, HRS and a SIS Technical Team. The respective applications' analyst within Information Technology Services will chair the teams. The applications end user is expected to solicit assistance for other members of the user community, as they deem appropriate to effectuate a successful recovery.

Equipment

a. The minimal equipment inventory required in the restoration process is as follows:

1. One OpenVMS AXP enterprise computer systems with ten gigablocks of disk storage and a tape deck;
2. One 600 LPM (lines per minute) data center printer;

3. Twenty network-ready personal computers with Windows 98 or higher.

b. Complete Inventory of Equipment housed in the ITS department.

See attachment 1. Compaq Service Agreement

Using the Backup Tapes to Recover The Systems

The Library vault has been rated as fire proof and disaster proof. To minimize the risk the monthly standalone backup tapes, the daily backup tapes and a copy of the post-production backup tapes are stored in the fire proof safe which is located in the Library. The pre- and post-production backup tapes are stored in the computer room. We anticipate using the contents of this vault to restore the systems for 95% of the disasters.

Monthly

The standalone backup is taken when a new system is put into production mode or when updates have been made to the operating system. This backup captures drive 0 which is where the system resides. These tapes are labeled including the date that the tape was made. When a system is destroyed, the most recent backup tapes, based on dates, are to be restored to the existing system DASD or to the newly acquired System and/or DASD. Once this standalone restore is completed, the system can now be activated (booted). The operating system will be used to restore the applications and associated data.

Daily

The daily backups are processed at the end of production. These tapes are labeled with identifiers denoting the day of the week the backup was taken. For example, the backup tapes for Monday will be labeled MON I to II since it takes two tapes to back up the system. The backup tapes are places in the vault located in the Charles Chesnutt Library. These tapes contain all of the applications and related data. The most recent copies of these tapes must be retrieved from either the computer room or the safe, located in the Library. Appropriate operating system commands are to be issued to add the contents of these tapes to the operating system environment. This task consists of a sequence of two (2) tapes and it will take approximately eight hours to complete. If the computer room is in tact, the latest set of post-production tapes can be used to bring the transactions current or current within one day.

Pre and Post Production Daily

It takes 1 tape for FRS and for SIS to be backed up. The tapes are labeled ZSS###. These tapes are stored in the computer room. An accurate record is kept which will allow one to know which tapes were used and what day the tapes were used. The decision on how to use these tapes resides with the appropriate Technical Teams.

EMERGENCY NOTIFICATION TELEPHONE LIST

Management Team	**Office**	**Home**
Vice Chancellor of Student Affairs Dr. Perry Massey	672-1469	
Vice Chancellor of Business and Finance Christopher Hinton	672-1151	
Chief Information Officer Arasu "Nick" Ganesan	672-1531	
Special Assistant to the Chancellor Dr. Booker T. Anthony	672-1141	

Damage Assessment		
Director, Information Technology Services Sarah Thomas	672-1918	
Assistant Vice Chancellor Facilities Maintenance, Planning and Construction Larry Blake	672-1431	
Facility Architect William Steve Martin	672-1431	
Plant Maintenance Supervisor Allen R. Williams	672-1431	
Electrician Supervisor David Abdul-Haaq	672-1880	
Network Manager Eric Silberberg	672-2552	
Safety Officer	672-1827	

Henry Brunson

Director of Public Safety & Chief of Police	672-1341
Chief Jerry Monroe	

Recovery

Director of Information Technology Services	672-1918
Sarah Thomas	
Administrative Systems Manager	672-1918
Ivan Williams	
Networking	672-2552
Eric Silberberg	

Recovery	**Office**	**Home**
Networking Computer Consultant	672-1909	
Wesley Prather		
Computer Operator	672-1198	
Linda Mitchell		
Computer Consultant	672-1912	
Emma Covington		
Plant Maintenance Supervisor	672-1431	
Allen Ray Williams		

Administrative Systems

Applications Systems Manager	672-1918
Vacant	

FRS

Information Technology Systems FRS Applications	672-1921
Antoinette Johnson	

Business and Finance	672-1084
Michelle Hall / Terry Merritt	
Budget & Payroll	672-1156
Tonya Jackson	

SIS

Information Technology Systems SIS Applications	
Vacant	
Student Accounts	672-1152
Terry Merritt	
Contracts & Grants	672-1084
Michelle Hall	
Financial Aid	672-1325
Lois McKoy	
Student Records	672-1181
Ivan Walker	
Admissions	
Charles Darlington	672-1371

HRS

Information Technology Systems HRS Applications Programmer	
Conroy Campbell	672-1917
Human Resources	
Doris Lane	672-1455

General

UPDATE

This plan will be reviewed and updated yearly. However, if changes occur which will impact the validity of the disaster recovery plan, then the plan will be updated at the time the change occurs.

Validating

Due to the cost associated with moving existing hardware or purchasing duplicate hardware, the testing of this plan will be limited to rebuilding the system and the recovery of the data files. If a disaster occurs and new hardware is required, the hardware vendor will have the responsibility to install the new hardware at the new location. This will be done by trained professionals.