James E. Shepard,
Founder

NORTH CAROLINA CENTRAL UNIVERSITY

Information Technology Services

Disaster Recovery Plan

November 2014

POWERED BY: NCCU ITS SERVICES TECHNOLOGY INFORMATION

ITS Disaster Recovery Plan history

Version Control

Version	Date	Author/Editor	Change Description	Comments
1.0	March 2002	Multiple	Original plan	
2.0	January 2005	Mary Lou Barlow	Edited three DRP's into one plan	
3.0	October/ November 2007	Steve Ornat	Updated with current ERP system and contact information	
3.1	December 2007	Steve Ornat	Updated contact information and create table/executive summary	
3.2	January 2008	Steve Ornat	Add new section	
3.3	February 2009	All	Edits to document	
3.4	November 2009	Harry Monds	Update entire plan	
4.0	April 2012	All	Update of entire plan	CIO and all directors updated the entire plan
4.1	April 2013	Steve Ornat	Updating of the entire plan with correct contact information	Changed tables and contact lists as needed
5.0	November 2014	Steve Ornat	Updating of the entire plan with correct contact information	Changed tables and contact lists as needed

Note The content of this manual will be updated on an annual basis.

Table of Contents

I. QUICK REFERENCE SUMMARY

A. Introduction

This manual contains a DISASTER RECOVERY PLAN (DRP) for North Carolina Central University (NCCU) Information Technology Services (ITS) at 1801 Fayetteville Street Durham, NC 27707. The ITS division has main offices physically located at 712 Cecil Street, Durham, NC 27707.

This Plan is primarily an operational manual for the Information Technology Services Disaster Assessment and Recovery Teams to follow when organizing, evaluating the extent of the destruction, and initiating actions to recover. The technical information included or referenced is essential. It is directed to the involved team members.

A disaster may affect part or all of the following:

- ITS personnel
- ITS system software and data
- ITS equipment
- ITS site and facilities
- User program files at ITS
- User applications data and documentation

The ITS division assumes responsibility for all of description as explained in this document.

System software, system data, and user program files for users at NCCU are backed up on computer tapes and stored in an off-site vault in the Registrar's Office in the Hoey Administration Building. These backup tapes could be used to restore the system on new equipment if so needed. Selected portions may be used to enable critical ITS user programs to be run at an alternative Data Center.

NCCU's ERP (Enterprise Reporting Program) Application called Banner, and associated applications are running in a "Hosted" environment at MCNC. The hosted environment is being managed by UNC General Administration (GA). In the event of a disaster at MCNC the recovery responsibility belongs to MCNC and UNC-GA. NCCU will play a support role in this effort. For a disaster that involves the NCCU campus, NCCU Information Technology Service has the primary responsibility for recovering the Information Technology Services for the campus users.

B. Disaster Preparedness Procedures

The purpose of this ***Quick Reference Summary*** to have in one location all of the key information needed in the event of an emergency.

- What to do in the event of an emergency
- Where to go in the event of an emergency
- Convening or meeting locations of the Response Teams
- Listing of Services and Applications used by NCCU

The vendors of equipment at the ITS Data Center have standard policies to assist customers after a disaster. The ITS Disaster Recovery Team has the responsibility for contacting the vendors to schedule recovery equipment.

The Chief Information Officer will be the source of primary assistance in the selection of a suitable permanent new site for ITS. Specific information about site and facility requirements and procedures for acquisition are described in this Plan.

C. Purpose and Scope

Management personnel of the University are responsible for protecting all assets of our organization. These assets include employees, physical property, information, and records relating to the conduct of the business.

The purpose of this plan is to have alternative arrangements for any operational critical systems and resources that would be necessary in case of a disaster in the main location of operation for Information Systems. Information Technology Support systems support staff are located on the third floor of the H.M. 'Mickey' Michaux New School of Education Building (SOE).

This Disaster Recovery Plan documents the procedures for recreating an operational Center for the users of ITS within a reasonable time and reasonable cost. The purpose of the Plan is to facilitate quick and orderly recovery of operations for ITS users. The Plan is fully applicable if destruction to all existing facilities is complete. Recovery from destruction of only some facilities or some system data is covered by selective portions of the Plan.

D. Critical Services and Applications currently in operation at NCCU

Critical Services and Applications				
pplication Name	Critical? Yes/No	Fixed Asset on NCCU's campus? Yes/No	Manufacturer	Comments
anner	Yes	No		
mail	Yes	Yes	Microsoft / Dell	*1,2,3 Exchange 2010 / Dell PE 1955 / NetApp SAN array
eb site	Yes	Yes	Microsoft SQL/CMS/CF	*1,2,3 Multiple systems / PowerEdge 2950/1955/Dell arrays
Mware, oduction nvironment	Yes	Yes	VMware / Dell	*1,2,3 VMware 4.0 ESXi, ESXi 5.0, ESXi 5.5, Dell PE1950, PE1955, PE2950, PE710R NetApp SAN array
ackboard	Yes	No		Hosted Services
NS	Yes	Yes	Microsoft	*1,2,3 VMware ESX5i, Dell PE 1955 x 2
HCP	Yes	Yes	Microsoft	*1,2,3 Dell PE 860
aglebus	Yes	Yes	NetVault / Overland Array	*1,2,3 Netvault backup, Dell PE 2850, Overland Tape VTL Library
ebmail	Yes	Yes	Microsoft	*1,2,3 Exchange 2010, Microsoft 2012 R2 Hyper-V cluster
ymantec: nti-Spam	Yes	Yes	BrightMail v6.	*1,2,3 Dell PE 1955 x 2
ymantec: nti-Virus	Yes	Yes	Anti-Virus v10.1/10.2	*1,2,3 Gateway 960
uminis	Yes	Yes	Sungard	*1,2,3 Luminus v3 – Account Creation
haros rinter server	Yes	Yes		*1,2,3 Student Printing services
ctive rectory	Yes	Yes	Microsoft	*1,2,3 Server 2003/2008/2012 Mixed-mode Domain
ouchnet	Yes	No		Credit Card Payment Gateway

Comment Legend:				All DR designated systems are backed up on a da weekly and monthly basis to VTL and/or Tape media. Back-Up Schedule: *1 = Runs daily* *2 = Runs weekly* *3 = Runs monthly*

II. DEPARTMENT VISION, MISSION AND GUIDING PRINCIPLES

A. Vision

ITS will work collaboratively to create an information technology environment which provides all students, faculty and staff direct and easy access to online tools and information sources; enabling the entire NCCU community to effectively accomplish their goals.

B. Mission

ITS is committed to supporting the NCCU community by providing direction, quality information technology resources and effective services to promote student success. We strive to create technological solutions that are timely, easy to use and relevant. Providing consistent, high quality and respectful customer service is of paramount importance. Through our efforts we must deploy technologies that will:

- Improve the operational effectiveness and efficiency of the administrators, faculty and staff at NCCU through the use of technology.
- Enhance the Research, Teaching and Learning process through the use of technology
- Provide adequate support of the technology that is deployed
- Ensure that technology and services provided are at lowest possible cost

C. Guiding Principles

Regardless of the population being served, or the IT services being provided, the management and staff of the Information Technology Division at NCCU have dedicated themselves to the following principles in all professional efforts.

- We will be above reproach in matters of ethics, legalities, and professional conduct.
- IT staff understands that the perception of our service is as important as the actual quality of the service, so we will strive to be courteous, civil and polite in all client contacts.
- In return, IT management will provide the IT staff with a work environment that is collegial and respectful of individual needs.
- Our goal is to achieve excellence in everything we do and we will endeavor to exceed the expectations of our clients.
- Finally, in matters of our clients' preferences, the staff will offer its professional opinion on the best method for delivery of quality services but, if disagreements arise, the bottom line metric is that the end user is always right.

III. DISASTER PLAN ATTRIBUTES

A. In the event of a disaster, the CIO or his/her designee will:

1. Notify the people listed on the Emergency Contact list; (See Appendix A)
2. Initiate organization of the teams;
3. Specify the immediate temporary team headquarters;
4. Direct the evaluation of destruction areas, which are listed in the "Damage Assessment Checklist"; (See Appendix B)
5. Coordinate all disaster recovery actions; and
6. Insure that the disaster history outlined in the "Disaster History Outline Requirements" section is maintained.

B. If telephone service is not available in the vicinity, then a messenger from the University Police will be dispatched to the homes of the team members: University Police will be provided with addresses and directions to the homes of the persons listed below.

1. Chief Information Officer
2. Director or Enterprise Information Systems
3. Director of Network Services & Telecommunications
4. Director of Audit Compliance and Business Continuity (Security and Compliance)
5. Director of User Support Services
6. Director of Web Services

C. Team Headquarters

1. The Team will locate in an available room in the School of Education, the Shepard Library (NOC) or a safe building nearest to the site of the destroyed Computer facility as directed by the CIO or his/her designee. If some salvage of on-site system support material is possible, Computer Labs in various building are alternatives.
2. If destruction of the site is total, the Team will locate in available rooms nearest to the alternative Computer facility as directed by the CIO or his/her designee.
3. Location of NCCU ITS operations are dependent on the conditions that caused the disaster and appropriate arrangements will be made and sites evaluated based on the conditions.

IV. PHYSICAL FACILITIES - REQUIREMENTS FOR A NEW DATA CENTER

A. Space Requirements

The Office of Fixed Assets at NCCU maintains information concerning available sites, both State and privately owned. The list of available sites changes frequently. The Office of Fixed Assets has indicated a willingness to aid in the acquisition of needed floor space should the need arise.

The person to contact at the Office of Property Management is:

Director of Fixed Assets (919) 530-7124

B. Floor Space Requirements

Computer Room	800 Square Feet
Tape Library	100 Square Feet
Staff Office Space	1,912 Square Feet
Conference Room	373 Square Feet
Paper Storage	800 Square Feet
Miscellaneous Storage	400 Square Feet

C. Total Electrical Service

The power requirements for an alternate computer facility are as follows:

Computer Equipment	1 - 200 Amp	3 phase service
Air Conditioners	2 - 100 Amp	3 phase service
UPS	1 - 65K VA	3 phase service (with a battery life, full load of 1 hour - minimum)
Generator	1- 65K VA	3 phase generator with manual transfer switch

The air conditioning requirements for a backup computer facility are as follows:

Computer Equipment	2 - ten ton units

V. DISTRIBUTION, REVISIONS AND TESTING OF THE DISASTER RECOVERY PLAN.

The disaster recovery plan for NCCU is distributed to members of the Disaster Recovery Teams as well as all members of the CIO's cabinet. A copy of the plan is maintained offsite. A disaster recovery test, whether a full exercise or a Table Top exercise should be conducted once a year.

A. Updating/Testing of the Plan

Copies of the Disaster Recovery Plan will be given to each of the following:

1. Chief Information Officer
2. Director of Internal Audit
3. Members of Chancellor's Cabinet
4. Members of the CIO's cabinet
5. Members of the Disaster Recovery Teams
6. Other campus units and constitutes that desire a copy of the plan

For safety, a copy of the Plan will be stored with the Enterprise Information Systems backup files and documentation located in the Registrar's Office fire-proof safe.

A copy of the Plan will be kept at the ITS reception area for ITS personnel to view if so desired.

Revisions in names, addresses, telephone numbers, equipment and other information in this plan will be made and distributed every year, if needed, to holders of the plan.

Note: Enterprise Information Systems conducts a partial test of its system backup each time a clone of production data base is performed and hence, a form of Disaster Recovery is done many times each year.

B. Disaster History Outline Requirements

In the event of a disaster, the Disaster Recovery Team is responsible for establishing and maintaining a record of all disaster recovery activities. The purpose of this history is to serve

as a record of events for subsequent reviews and debriefings with government agencies, insurance companies, vendors, suppliers, and attorneys, et al. The history record will include, but is not limited to:

1. Chronological log of the disaster event;
2. Chronological log of the recovery steps;
3. Analysis of cause of disaster;
4. Man-hours and dollars expended by recovery tasks;
5. Impact of business interruptions;
6. Conclusions with respect to ways, in which, business interruption and/or cost could have been reduced; and
7. Recommendations to minimize impact of future disasters.

VI. NCCU INFRASTRUCTURE, EQUIPEMENT AND SERVICES

A. Networking and Telephone Equipment:

1. Networking routers and switches are operated by NCCU ITS as part of the Network Service and Telecommunications Department.

2. The Campus Telephone system is owned and operated by State Government, the Office of ITS. This State Agency is responsible for the operation, upgrades and repair of the telephone system located on the campus of NCCU.

B. Networking and Support to Campus Facilities

The department of Networking and Infrastructure provides and supports an Optical Fiber based system that connects all of North Carolina Central University's buildings. The Shepard Library Network Operations Center (NOC-S) contains several networking routers and switches that support all the buildings on the campus of NCCU. The main core routing/switching devices are redundant Cisco 6509 switches with Gigabit Ethernet and 10Gigabit Ethernet backbone networks. The backbone networks connect to the remote buildings that comprise the NCCU campus. The two core devices are in place to provide redundant connections to the majority of campus buildings, with the exception of very small buildings, with dual optical fiber connections going to each core router. In the event one of the core devices fails, the standby core device will support the campus building. These core devices are configured in an arrangement with an automated system that checks the condition of the building network once a second and in the event of an optical fiber or system failure the core routers are prepared for "Hot Standby switch over" so that the remote buildings are not without network support.

C. Connection to the Internet:

NCCUNET's connections to the Internet were installed and are maintained by North Carolina Research and Education Network (NCREN).

D. Pathway for NCCU's internet connection

1. The Primary Gigabit connection to NCREN enters the campus at the corner of Alston Avenue, Highway 55 and Cecil Street via Duke Net optical fiber. The optical fiber is terminated in the H. M. Michaux New School of Education Building Network Operations Center, which is located on the third floor of the H. M. Michaux New School of Education Building, room 3036. The fiber path is cross-connected between the H. M. Michaux New School of Education Building Network Operations Center and the Network Operations Center in the Shepard Library. The final termination of this

connection is the Shepard Library Network Operation Center. There are multiple strands for optical fiber between the Network Operations Center in the H. M. Michaux Education Building and the Network Operations Center in the Shepard Library. These optical fibers are used to connect the NCREN connection to the core routers located in the Network Operations Center in the Shepard Library.

2. Redundant Internet Path is terminated in the Latham Parking Deck Telecommunications entrance Facility.

E. Generator backup power:

The backup generator powers the essential networking equipment. The backup generator has a fuel tank that supports the NOC-S for up to three (3) days. If there is an extended power outage the backup generator will be refueled making the risk of loss of networking equipment non-existence. This makes the risk of extended Utility power outages of minimal concern.

It is the responsibility of the Physical Plant to provide regular testing of the generator and provide coordination with the office of Networking, Infrastructure and Operations to ensure that the generator fuel tank is kept full during extended utility failure.

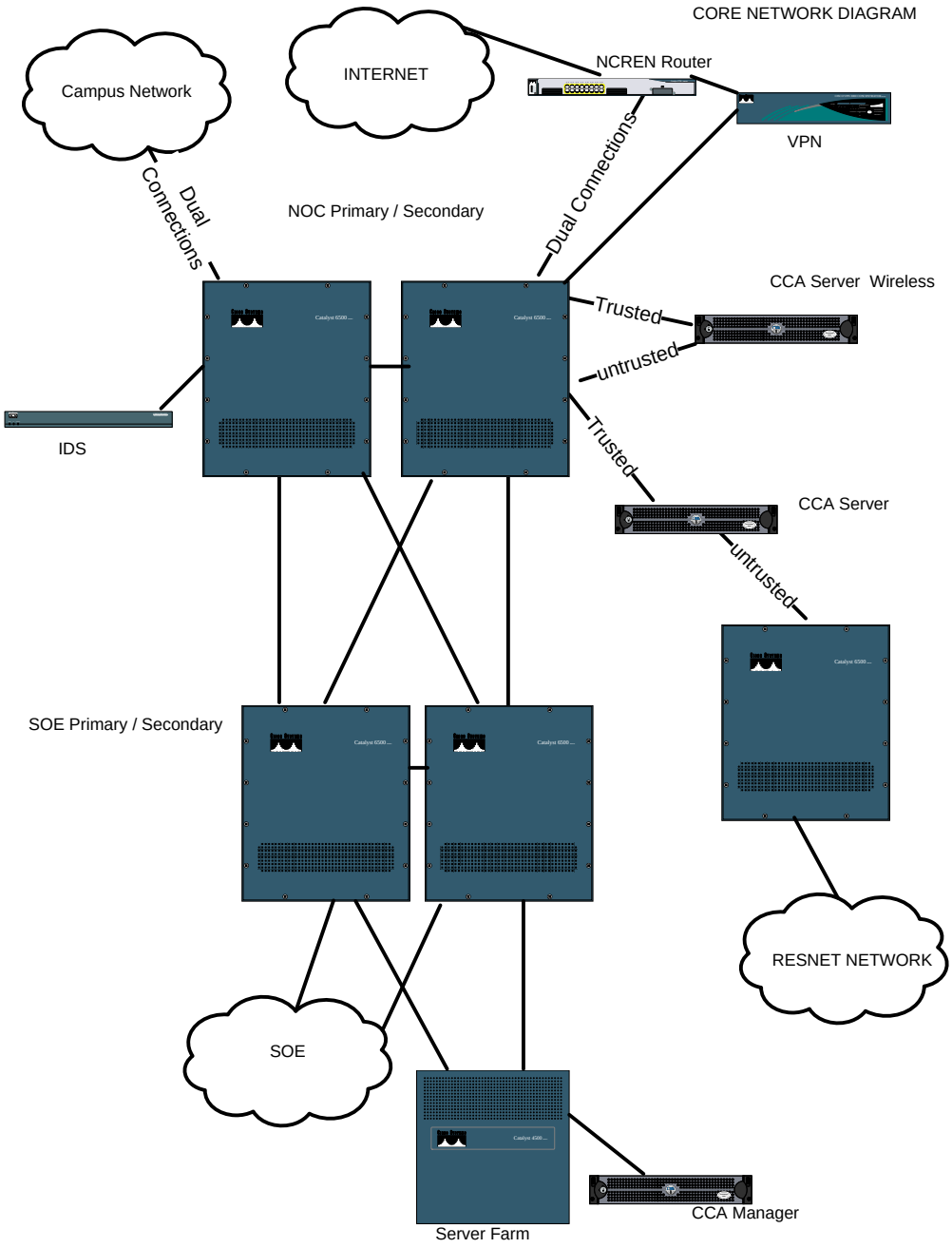
F. UPS backup power:

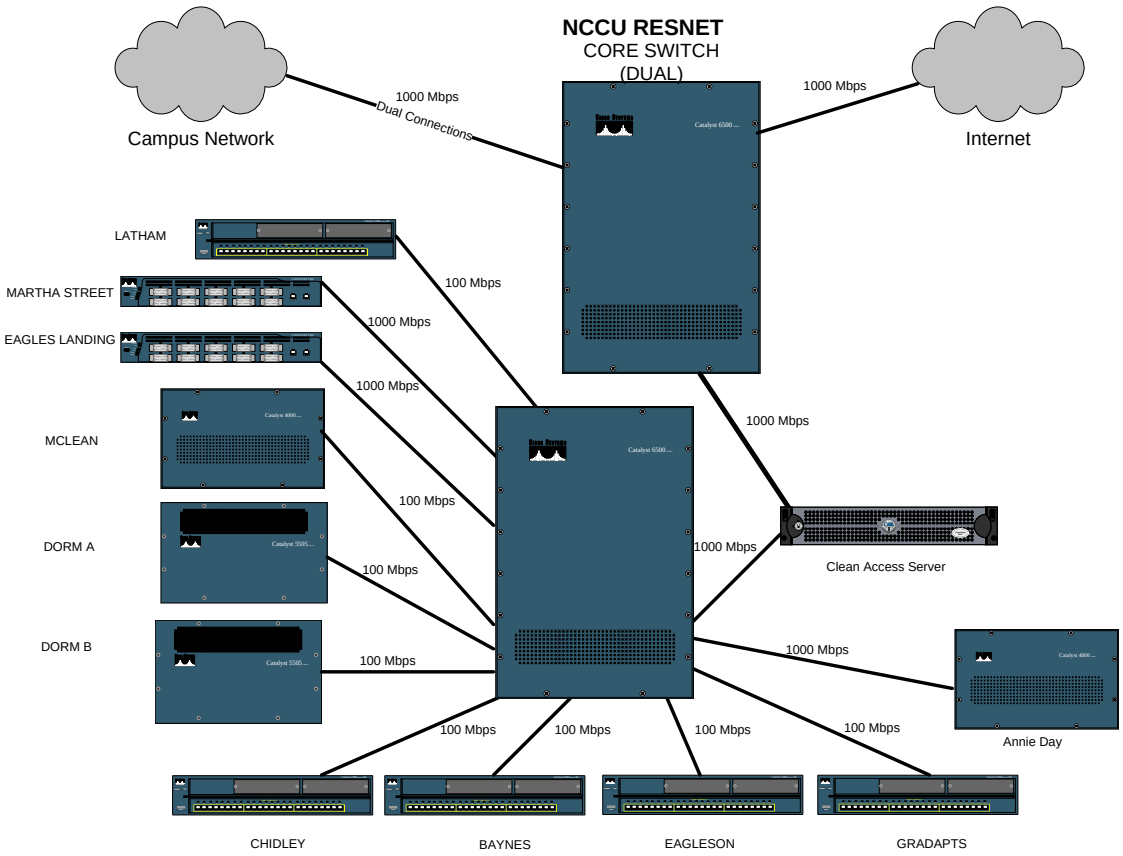
The UPS unit will provide a minimum of one (1) hour of backup battery power support of all the essential networking equipment. In the event of failure of Public Utility as well as failure of generator power the UPS system would be fully utilized.

G. Physical Security:

A list of who has access to the NOC-S is posted on the two (2) entrance doors that service the Network Operations Center.

H. Network Diagrams




NCCU RESNET
CORE SWITCH
(DUAL)
Campus Network
1000 Mbps
Dual Connections
1000 Mbps
Internet
LATHAM
MARTHA STREET
EAGLES LANDING
MCLEAN
DORM A
DORM B
100 Mbps
1000 Mbps
1000 Mbps
100 Mbps
100 Mbps
100 Mbps
1000 Mbps
1000 Mbps
Clean Access Server
1000 Mbps
Annie Day
100 Mbps
100 Mbps
100 Mbps
100 Mbps
CHIDLEY
BAYNES
EAGLESON
GRADAPTS

Network Operation Center @ H.M. Michaux Education Building (NOC-SOE)

Redundant Network Operation Center:
The department of Networking and Infrastructure has put in place additional network routers to support the campus as a "redundant NOC." This redundant NOC will provide networking services to mission critical campus buildings in the event the Shepard Library Network Operation Center (NOC-S) are damaged or destroyed.

The H. M. Michaux New School of Education Building was configured for the main purpose of providing the campus with the redundant Network center and redundant entrance of Networking, Infrastructure and Operations services to the entire campus.

The H. M. Michaux New School of Education Building is located at the farthermost South Eastern corner of the campus. This location is on the right-of-way for Verizon telephone lines as well as Optical fiber from DukeNet and Time Warner. In addition, unused infrastructure in the form of manholes and conduit was installed from the H. M. Michaux New School of Education Building toward Alston Avenue, Highway 55.

Core network Switches and Routers
The NOC in H. M. Michaux New School of Education Building (NOC-SOE) contains dual Core routers to mirror the operation of the Shepard Library Network Operations Center. The NOC-SOE is also equipped with ethernet switches for the operation of the network within the School of Education.

Generator backup power
The backup generator also powers the essential networking equipment. The backup generator has a fuel tank that supports the NOC-SOE for up to three (3) days. If there is an extended power outage the backup generator will be refueled making the risk of loss of networking equipment minimal.

It is the responsibility of the Physical Plant to provide regular testing of the generator and provide coordination with the office of Networking, Infrastructure and Operations to ensure that the generator fuel tank is kept full during extended utility failure.

UPS backup power
The UPS unit will provide a minimum of one (1) hour of backup battery power support of all the essential networking equipment. In the event of failure of Public Utility as well as failure of generator power the UPS system would be fully utilized.

Physical Security:

A list of persons that have access to the NOC-SOE is posted on the two (2) entrance doors that service the Data and Network Operations Center.

Remote Building Facilities
Each building on the campus of NCCU contains an "Equipment Room (ER)" or "Building Distribution Facility (BDF)."

Each remote building Equipment Room consists of a Building Entrance switch. The Building Entrance switch is connected back to the Shepard Library Network Operations Center (NOC-S) via buried optical fiber. The speed in which the remote buildings connect back to Shepard Library Network Operations Center (NOC-S) is either Fast Ethernet (100 Mbps) or Gigabit Ethernet (1000 Mbps.)

The building entrance switch either supports the local users via directly connected connections using the copper cabling within each building. In some remote buildings, local Ethernet switches are located on individual floors and the local users are directly connected on the user's floor.

Telephone Support to Campus Facilities
The State of North Carolina office of ITS Telecommunication Services, manages the campus voice communications system. NCCU ITS in conjunction with State ITS are responsible for all adds, moves, and changes to telephones State ITS provides the system maintenance and all service issues for the campus PBX.

Outages to individual telephones are handed on the next business day or the next day. ITS State Telecommunication Services handles Service issues affecting an entire building or the campus.

The system is supported by a state contract that the State of North Carolina office of ITS, Telecommunication Services holds with the telephone company Embarq.

Location of Telephone System
The NCCU Campus is supported by an Option 81C Nortel telephone system otherwise known as a PBX (Private Branch exchange.)

This telephone system is located within the Network Operations Center in the Shepard Library (NOC-S)

Generator backup power

The backup generator provides power to the Telephone system in the event of a failure of utility power. The backup generator has a fuel tank that supports the NOC-SOE for up to three (3) days. If there is an extended power outage the backup generator will be refueled making the risk of loss of networking equipment non-existence.

UPS backup power

UPS units that provide between 45 minutes and 1 ½ hour of backup battery power support of all the essential networking equipment. In the event of failure of Public Utility as well as failure of generator power the UPS system would be fully utilized. This UPS is part of the system that State ITS maintains. Testing is part of their agreement with Embarq.

Physical Security

A list of who has access to the NOC-S is posted on the two (2) entrance doors that service the Network Operations Center.

Equipment Listing

Networking, Infrastructure and Operations does not have a contract with an outside vendor for a "replace all" or "recover all" contract. Networking, Infrastructure and Operations keeps spare parts in two main locations on campus. Parts are housed in room #3 of the Old Health Building as well as rooms 3032 and 3033 within the new School of Education.

Networking, Infrastructure and Operations has business relationships with networking vendors and replacement equipment can be acquired in the matter of a few hours to a few days in the event of an emergency by issuing an emergency Purchase Orders.

Vendor List is located in Appendix XIII – Vendors

Contingency Plans

The main hub of all data and telephone activities is located in the Shepard Library Network Operations Center. This Network Operations Center contains all the optical fiber to each building on the campus of NCCU. If this Network Operations Center were involved in a disaster and the Network Operations Center is destroyed, networking as well as telephone services to campus building would be interrupted.

Emergency Contingency Plans

An emergency purchase order can be placed with the optical fiber contractor to restore the optical fiber patch panels as well as the optical fiber in any other building affected by the disaster

In place of the creation of an emergency purchase order, NCCU will use the convenience contract that the State of North Carolina has in place with a Category "A" wiring contractor. Vendor List is located in Section VII – Vendors

Telephone PBX Contingency Plan:
In the event of a disaster involving the Telephone PBX the following two (2) scenarios were prepared by State of North Carolina office of ITS, Telecommunication Services.

Disaster Recovery Scenario 1: In this scenario the entire Shepard Library NOC has been destroyed including fiber and copper wire distribution frames within the NOC.

Under this scenario new trunk facilities would be provisioned from State ITS and terminated within the Hoey Administration Building utilizing the existing NCCU copper entrance facilities of which 90% are available for use. A standby Meridian PBX would be brought in by Embark Communications and placed in the basement of Hoey and connected to the existing building wiring restoring phone service to the main administrative building. At least (2) temporary phone service lines (analog) would be placed in each outlying campus building to provide service to all campus buildings. A combination of existing in-ground wiring and temporary cabling placed on the ground would be used to extend service from the Hoey Administration Building to the entire campus. Up to 400 lines could be returned to service in the first 48 hours.

Disaster Recovery Scenario 2: In this scenario the Shepard Library NOC is intact including fiber and copper wire distribution frames, however, the Meridian PBX has been destroyed and the NOC is no longer suitable for placement of a temporary Meridian System.

Under this scenario new trunk facilities would be provisioned from State ITS and terminated in the H. M. Michaux New School of Education Building. A standby Meridian PBX would be brought in by Embark Communications and placed in the network room of the H. M. Michaux New School of Education Building. Using the existing fiber from H. M. Michaux New School of Education Building and through the Shepard Library fiber remote shelves would be placed in critical areas around campus to return service to Hoey Administration and other key buildings around campus. Up to 2000 lines could be returned to service within the first 48 hours.

Service and backup agreements with outside vendors:

Cisco Systems Inc.:
NCCU has an agreement with Cisco Systems Inc. to provide telephone technical support and Next Business Day equipment. This allows NCCU Networking, Infrastructure and

Operations staff 24 hours a day and 7 days a week and 365 days a year, telephone technical support. This agreement also states that Cisco Systems will replace any failed equipment by the next business day. We use this any time a piece of Cisco hardware fails and Cisco sends us a replacement. We have Cisco Smartnet that commits to replacement parts NBD (Next Business Day.)

North Carolina Research and Educations Network (NCREN):
NCREN is a private non-profit origination that provides State wide intranet access as well as Internet access to all Universities in the entire UNC system. They also provide access to other State agencies.

NCCU has an agreement with MCNC that states their intention to provide required services to support NCCU in the recovery from a disaster.

In the event that the disaster is total at NCCU, users will reply on their Business Continuity Plans until IT services are restored.

VII. EQUIPMENT

All computer equipment is listed in Appendix C.

A. Application priorities

The order of work priority is kept flexible to accommodate ad hoc priority work requests received from the Chancellor, Vice Chancellors and Chief Information Officer. In general, the following priority is utilized.

1. Finance
    a. State Reporting
    b. Payroll Interface operations
    c. Cash Receipts Interface
    d. Telephone Billing System
    e. Agency Invoice
2. Banner
    a. Admissions
    b. Student Records (SR)
    c. Financial Aid Management (FAM)
    d. Billing & Receivables (BR)
    e. Student Data File
    f. HR Datamart
    g. Student Housing(RMS)
    h. Library Fines
    i. Interactive Voice Response (IVR)

j. Self Service Banner (SSB)
k. Internet Native Banner (INB)

3. Personnel Data File
4. Human Resource Systems (HRS) Leave Reporting- Is this not part of Banner

All applications listed above are mission critical. Critical operation periods are determined by the data owners. In general, registration, grading, billing, and financial month-end/year-end close are always critical times.

B. Systems Documentation

C. Administrative Systems

D. Student Information Systems

a. Admissions
b. Student Records
c. Financial Aid Management
d. Billings and Receivable
e. Student Data File
f. Student Housing
g. Library Fines
h. Interactive Voice Response

2. Financial Records Systems
   a. Financial Accounting
   b. Accounts Payable
   c. Purchasing
   d. Fixed Assets
   e. Accrual System
   f. State Reporting
   g. Payroll Interface
   h. Cash Receipts interface
   i. Telephone Billing System
3. Business and Auxiliary services including the CS Gold data system
4. EPA/SPA Data File
5. Human Resources System on the Banner system (HRS) and PMIS system hosted by the North Carolina Office of State Personal (OSP). This includes leave Reporting

E. Off-Site Backup of System Recovery Tapes

****** In order for "tape backup" recoveries to proceed, the NetVault back-up system must be restored first, requiring the software to be installed and a tape drive that is capable of reading/writing to LTO-3 tape media be available. ******

System Administrators back-up to disk drives onto tape media rotated through an off-site storage location in the Registrar's. The procedure for all backup of disks is as follows:

Administrative Systems operators will rotate tapes each week provided for backup. A master backup schedule with tape numbers is provided in the tape Library and in the off-site storage area. This allows all concerned to be able to identify tape sets by day, by weeks, by tape numbers and by application.

VIII. OPERATIONAL PROCEDURES

A. Disaster Recovery Teams

The Disaster Recovery Plan will be carried out by four teams:

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

B. Management Team

If a "disaster" occurs that disables NCCU's computing and networking services, the Management Team will be responsible for the disaster recovery process. The group will direct the establishment of 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 procedures and processes outlined in their Business Continuity Plans.

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 Management Team will be chaired by the Chief Information Officer (See Management Team members in Appendix A). The Chancellor and his Cabinet will be kept up-to-date on the extent of the damages and the recovery process by the CIO. A recovery schedule will be developed by the Recovery Team for review and

approval by the Management Team. The Recovery Team will then execute the plan.

C. Damage Assessment Team

The process for determining the extent of the disaster and what is required to re-establish the Data Center Computing and Networking Services is as follows:

The operation staff who becomes aware of a problem will notify the Chief Information Officer and the Director of User Support Services that a disaster has occurred which disabled the computing and networking services. If no operations personnel is on duty, the University Police will notify the Chief Information Officer who will in turn notify the Director of User Support Services (or on-site ITS Director) so he can assemble the Damage Assessment Team. The Chief Information Officer will also notify 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 intact. Efforts will be undertaken to provide access to the off-site storage vault in case some of the contents are needed for the recovery of the Data Center.

2. The Director of User Support Services (or on-site ITS Director) 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 User Support Services will assemble the Recovery Team instead of the Damage Assessment Team.

Damage Assessment

- If operations staff were on duty, the status of personnel will be determined. Immediate notification will be given to the Chief Information Officer 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 Banner (and its required ancillary applications). If access to the Data Center is denied due to the extent of damages, this team will terminate all efforts and the Recovery and the Management Teams will be notified.

D. Recovery Team

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 Data Center and the campus-wide networking infrastructure to a base-line functional capability. The team will also review the inventory of critical resources including but not limited to NCCU developed application documentation, operating systems manuals, hardware and computer systems manuals to ensure completeness. 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 which 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 (based on their documented Business Continuity Plans) 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 Data Center and other computing resources.

E. Technical Assistance Team

After the system is restored, the Technical Team will determine the state of transactional processing. 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 (again, based on their specific Business Continuity Plans) and keep an accurate account of all transactions. When the system has been made operational, the 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 Enterprise Systems Applications Analysts and key end users will staff this group. The applications end user is expected to solicit assistance from other members of the user

community, as they deem appropriate to ensure a successful recovery.

IX. APPROVALS

_____	_____
Leah Kraus, Chief Information Officer	Date
_____	_____
Robert Gains, Interim Internal Auditor	Date
_____	_____
Debra Saunders-White, Chancellor	Date

Submitted By: **Steven M. Ornat, RCDD**

X. APPENDIX A: ITS EMERGENCY CONTACT LIST

Staff/Title	Member of teams	Contact Information	Responsibility
Leah Kraus, Chief Information Officer	Management Team Damage Assessment Team	Office Phone: 919-530-7488 Cell Phone: 336-908-6977	Direct ITS Emergency personnel
Bob Northcott Director of Campus Support Services	Management Team Damage Assessment Team Recovery Team	Office Phone: 919-530-6364 Cell Phone: 770-630-2939	Monitors and restores student labs, campus communications, media services
Donald Nolen Director of Enterprise Systems and Application Development	Management Team Damage Assessment Team Recovery Team Technical Team	Office Phone: 919-530-5350 Cell Phone: 919-943-0596 Home Phone: 919-767-8077	Monitors and restores ERP systems Monitors and restores servers
Joel Faison Director of Networking and Telecommunications	Management Team Damage Assessment Team Recovery Team	Office Phone: 919-530-6919 Cell Phone: 919-885-3455 Cell Phone (Personal): 919-247-0725 Home Phone: 919-326-2275	Monitors and restores telephony and campus networks.
Steve Ornat Director of Audit Compliance and Business Continuity		Office Phone: 919-530-7171 Cell Phone: 919- Home Phone: 919-542-5994	Compliance to the controls that have been put in place
Patrice Parrish Director of User Services	Damage Assessment Team Recovery Team	Office Phone: 919-530-6780 Cell Phone: 919-943-0741 Home Phone: 919-596-3808	Maintains campus communications, help desk services
Damond Nollan Director of Web Services	Damage Assessment Team Recovery Team Technical Team	Office Phone: 919-530-6399 Cell Phone: 919-724-5647	Restore web services
Joel Director of Networking and Telecommunications	Damage Assessment Team Recovery Team Technical Team	Office Phone: 919-530-6364 Cell Phone: 919-885-3455 Cell Phone (Personal): 919-247-0725 Home Phone: 919-326-2275	Restore server and e-mail connectivity
Joel Director of Networking and Telecommunications	Damage Assessment Team Recovery Team	Office Phone: 919-530-5096 Cell Phone: 919-885-3455 Cell Phone (Personal): 919-247-0725 Home Phone: 919-326-2275	Restores telephony and networking services

XI. APPENDIX B: DAMAGE ASSESSMENT CHECKLIST

ITEM	REQUIRED REPAIR REPLACEMENT ACTION	PERSON ASSIGNED RESPONSIBILITY	PLANNED COMPLETION TIME/DATE
Building Structure			
Access to Building			
Computer Facilities			
Power			
Electrical Distribution System			
Heating, Ventilation & Air Conditioning (HVAC)			
Flooring			
System C02			
Computer Equipment			
Tape Library			
Tapes			
Documentation On-Site in Staff Offices			
Telephone Equipment			
Office Equipment			

XII. APPENDIX C: SERVER LOCATION LIST

SERVER NAME	Owner/Primary Admin	Model	Applications and Services	Operating System	Inventory Notes
AV Server1	CNash	Gateway 980	Symantec Anti-Virus Server	Windows 2003 R2 Ent. Edt. SP2	
BANAPP-SRV1	Jaya / Dnolan	Sun SunFire V240	Sun OS	SunOS	
BES05		Dell PowerEdge 1955	BES 5.0 Enterprise	Windows 2003 R2 Ent. Edt. SP2	SOE - Chassis01 - 92H14C1
CMS1	Dnollan / Dliboon	Dell PowerEdge 2950	Content Management Software - Main server, ColdFusion 7 Enterprise	Windows 2003 R2 Ent. Edt. SP2	
DailyDB	Jaya	Sun Fire V240	SunOS	SunOS	
DC1		Dell PowerEdge 2850	Active Directory Domain Controller ADS - Global Catalog Server Holds all FSMO Roles DNS Services (Secondary) NTP	Windows 2003 R2 Ent. Edt. SP2	
DES01	Dliboon	Dell PowerEdge 1955	VMware ESX 3.5i U3	VMware ESX 3.5i U3	SOE - Chassis03 - G9V22D1
DES02	Dliboon	Dell PowerEdge 1955	VMware ESX 3.5i U3	VMware ESX 3.5i U3	SOE - Chassis03 - G9V22D1
DHCP1-PE860	CMartin	Dell PowerEdge 860	DHCP Server	Windows 2003 R2 Ent. Edt. SP2	
Direct Deposit - (State FTP)	Dnolan	Dell OptiPlex GX620	SFTP service to NC State Comptroller - fed via Banner	Fedora	Back Room
DNS01	Dliboon	VM on DES01	Primary External DNS server	Windows 2003 R2 Ent. Edt. SP2	VM on DES01
DNS02	Dliboon	VM on DES02	Secondary External DNS server	Windows 2003 R2 Ent. Edt. SP2	VM on DES02
EAGLEBUS		Dell PowerEdge 2850	Netvault Backup Server. HP Storage Works	Windows 2003 R2 Ent. Edt. SP2	
EARTH	Dnolan	Sun Fire V440	SunGard SCT Banner ERP Banner Database Test. Additional Apps: Server/Development, Oracle RDBMS 9.2.0.6.0	SunOS	
EQUALLOGIC SAN		Equallogic PS200E (14 array devices)	iSCSI Storage Area Network	N/A	
ESX03	DLiboon	Dell PowerEdge 1950	Vmware ESX 3.5 Enterprise	Vmware ESX 3.5 Enterprise	
ESX04	DLiboon	Dell PowerEdge	Vmware ESX 3.5 Enterprise	Vmware ESX 3.5 Enterprise	

		1950			
EXCH-CAS1		Dell PowerEdge 1955	Client Access Server (OWA, POP3, IMAP4 and Outlook), Hub transport Roles	Windows 2003 R2 Ent. Edt. SP2 x64	SOE - Chassis01 - 92H14C1
EXCH-HT1		Dell PowerEdge 1955	Hub Transport Server (Routes all mail)	Windows 2003 R2 Ent. Edt. SP2 x64	SOE - Chassis01 - 92H14C1
Exch-MB1	SNixon	Dell PowerEdge 1955	Mailbox Server Faculty/Staff A-J	Windows 2003 R2 Ent. Edt. SP2 x64	SOE - Chassis01 - 92H14C1
Exch-MB2	Dliboon	Dell PowerEdge 1955	Mailbox Server Faculty/Staff K-Z	Windows 2003 R2 Ent. Edt. SP2 x64	SOE - Chassis01 - 92H14C1
Flow03		VM on DES01	Symantec Brightmail AntiSpam Mail Security - Mail Relay	Windows 2003 Ent. Edt. R2 SP2	VM on DES01
Flow04		VM on DES02	Symantec Brightmail AntiSpam Mail Security - Mail Relay	Windows 2003 Ent. Edt. R2 SP2	VM on DES02
FS-1		Dell PowerEdge 1955	Windows File Server - User Home M: Directories	Windows 2003 R2 Ent. Edt. SP2 x64	SOE - Chassis02 - 5CKJ3D1
FS-2	Dliboon	Dell PowerEdge 2950	Windows File Server - Department Common O: Directories.	Windows 2003 R2 Ent. Edt. SP2	
FS-3		Dell PowerEdge 1955	Student file server / Unix to Banner NFS service	Win2K3 x64 Ent. Ed. R2 SP2 x64	SOE - Chassis02 - 5CKJ3D1
IDP-PROD-N01	Dliboon	VM on ESX105	Shiboleth IDP (C:\shibboleth)	Windows 2003 Std. Edt. SP2	VM on ESX105
IDP-PROD-N02	DLiboon	VM on ESX03	Shiboleth IDP (C:\shibboleth)	Windows 2003 Std. Edt. SP2	VM on ESX03
INB1-A	Dnolen / Snixon	Dell PowerEdge 1955	INB - Network Load Balanced	Win2K3 x64 Ent. Ed. R2 SP2 x64	NOC - Chassis - 8C7H3D1
INB2-A	Dnolen / Snixon	Dell PowerEdge 1955	INB - Network Load Balanced	Win2K3 x64 Ent. Ed. R2 SP2 x64	NOC - Chassis - 8C7H3D1
MYNCCU	Snixon	VM on VMAPP01	Production Luminus - banner link	Windows 2000 SP4	VM on VMAPP01
NAV01	CNash	Dell PowerEdge 1955	New Primary Symantec Anti-Virus Server & Mgmt. Console	Windows 2003 R2 Ent. Edt. SP2	SOE - Chassis02 - 5CKJ3D1
NEO 4100 (Tape Drives)		NEO Tape Drives	Netvault Backup / Overland	N/A	
NEPTUNE	Dnolen	Sun Fire V880	Banner, APPWorx	SunOS	
ODS	Dnolen	Sun Fire V440	Reports	SunOS	
ORASRV1	Dnolen	Sun Fire V440	Test Server Oracle 10g R2	SunOS	
PHAROS		Dell PowerEdge SC1425	Print Server.	Windows 2003 R2 Ent. Edt. SP2	
PS-1	SNixon	Dell PowerEdge	Windows Print Server: Primary	Windows 2003 R2 Ent. Edt. SP2	

		2950			
PS-2	Dliboon	VM on ESX03	Windows Print Server: Secondary	Windows 2003 R2 Ent. Edt. SP2 x64	VM on ESX03
Reo 9000 (Overland)		Overland Storage Reo 9000	iSCSI Disk Based Backup Unit for Storage Area Network	N/A	
SG-ADAP	Dliboon	VM on ESX04	Luminis ADAP web service (C:\ADAP\)	Windows 2003 R2 Ent. Edt. SP2	VM on ESX04
SG-Workflow	Creaves	Dell PowerEdge 1950	SunGard	Windows 2003 R2 Ent. Edt. SP2 x64	
SQL-SRV1	Dliboon	Dell PowerEdge 1950	MS SQL Server 2005, MS Visual Studio 2005,	Windows 2003 R2 Ent. Edt. SP2	
SRV-1		Dell PowerEdge 2850	Active Directory Domain Controller ADS - Global Catalog Server Holds all FSMO Roles DNS Services (Secondary) NTP	Windows 2003 R2 Ent. Edt. SP2	
SERVER NAME	**Owner / Primary Admin**	**Model**	**Applications and Services**	**Operating System**	**Inventory Notes**
SRV-2		Dell PowerEdge 2850	Active Directory Domain Controller ADS - Global Catalog Server Holds all FSMO Roles DNS Services (Primary) NTP	Windows 2003 Ent. Edt. SP2	
SSB01		Dell PowerEdge 1955	SSB	Windows 2003 R2 Ent. Edt. SP2 x64	SOE - Chassis02 - 5CKJ3D1
VCS (Virtual Center Server)		VM on ESX03/04	Virtual Center Server - ESX 3.5	Windows 2003 R2 Ent. Edt. SP2	VM on ESX03/04
Web-4	Dnollan / DLiboon	Dell PowerEdge 2850	W2K3 Ent. Edt, IIS 6.0, PHP 5.2.4	Windows 2003 R2 Ent. Edt. SP2	
Web Event	Dliboon	VM on ESX105	Active Data Calendar 3.6.0 (C:\websites\calendar\), IIS	Windows 2003 R2 Ent. Edt. SP2	VM on ESX105
Webfocus		Sun Fire V240	Webfocus	SunOS	Webfocus
WKFLW	Creaves	VM on Virtual-2	SunGard	Windows 2003 R2 Ent. Edt. SP2	VM on Virtual-2

XIII. APPENDIX D – VENDOR LIST

Vendor Name	Type	Contact Person	Telephone Information
Alphanumeric	Gold Support	Brenda Mai	919-376-4594
Appworx	Appworx/ UC4 Applications Mgrs.	Dalene Hayes	425-644-2121 x118
Axent Technologies, Incorporated			801-227-3700 800-222-0623 801-227-3703
BakBone 9540 Towne Centre Drive Suite 100 San Diego, California 92121		Joseph Gallo	561-488-7916
Blackboard Inc.	Blackboard		202-463-4860 or 727-848-8877
Cisco Reseller NWN Inc.	Networking routers, switches and wireless	Molly MHildebrandt@nwnit.com	919-653-4440 (Office) 919-539-8298 (Cell)
Cisco Systems Inc.	Networking routers, switches and wireless	Scott Wertz swertz@cisco.com	919-392-5035 (Office) 919-608-7801 (Cell) 919-7881299 (Fax)
CollegeNet	R25 Banner Interface	Yumi Burghart	503-973-5200
Dell	PC Lease	Gyneshwar	800-289-3355 ext. 53-77430
Dell Computer Corporation One Dell Way Round Rock, Texas 78682			800-625-8286 Fax 800-365-5329
DLT Solutions	TOAD Software Licenses	Debby Tendall	252-355-0261
Equallogic 9 Townsend West Nashua, NH 03063			HQ: 603-579-9762
Evisions	Intellecheck	Linda Doring	949-833-1384 x247
Information Builders	Webfocus Report Developer		212-736-4433
MCNC/NCREN	Internet connection	Network Operation Center trouble@ncren.net	919-248-1111

Micro Focus	Micro Focus		301-838-5184
Nortel Wireless / Pomeroy.	Wireless network	Marvin Gibson MGibson@pomeroy.com	704-293-0053 (Cell)
Numara	Asset Manager	Jennifer Lai	800-222-0550 x8968
Oracle http://metalink.oracle.com User name and password required to access support			
Oracle	Oracle Maintenance		866-868-3746
Overland Storage Inc. 4820 Overland Avenue San Diego, California 92123			800-729-8725
Process Software	Process Software Multinet Agreement	Byron Johnson	
Sprint Wireless	Cellular Telephones	Marilyn Blanchard marilyn.blanchard@sprint.com	919-868-0013 (Cell)
State ITS	Telephone System	Helpdesk its.incidents@ncmail.net	919-754-6000
SungardHE	Banner Maintenance	Hermey Schlesinger	561-392-7899
Touchnet	Touchnet Payment Gateway	Rachael Taggart	913-599-6699
University of North Carolina General Administration	Remote DBA		919-962-1000
VeriStor 3308 Peachtree Industrial Blvd Suite 110 Duluth GA 30096		Steve Bishop	
Veristor	SAN Maintenance	April Pitts	678-617-2696
Verizon Wireless	Cellular Telephones	Jeff Gleichauf Jeffrey.Gleichauf@VerizonWireless.com	919-740-5200 (Cell)

XIV. APPENDIX E – KEY TEAM PERSONNEL

A. Management Team

Title

Chief Information Office

Director of Enterprise Systems

Director of Infrastructure and Network Services

Physical Plant Director

VC and Chief of Staff

Vice Chancellor of Administration and Finance

Vice Chancellor of Student Affairs

Human Resources

Student Health Services

B. Damage Assessment Team

Director of User Support Services

Physical Plant Director

Director of Enterprise Systems

Director of Network Services and Telecommunications

Health and Safety Manager

Chief of Police

C. Recovery Team

Director of User Support Services

Physical Plant Director

Director of Enterprise Systems

Director of Network Services and Telecommunications

Health and Safety Manager

Chief of Police

D. Technical Team

Security Coordinator

Systems Programmer

Applications Programmer

Administration and Finance

Information Systems Applications Analyst SIS

Student Accounts

Financial Aid

Registrar

Admissions