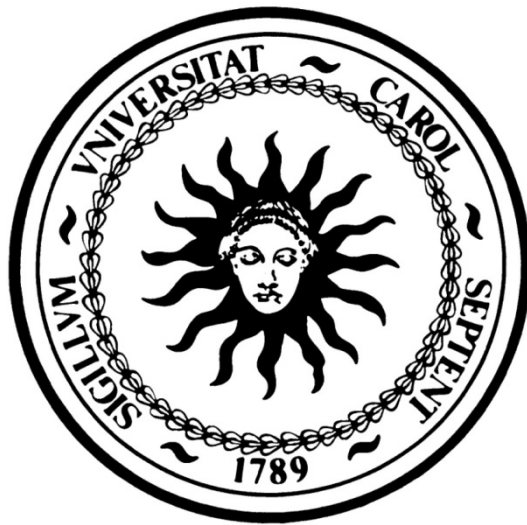


# UNC-GA

*Information Resources Division*

## Disaster Recovery Plan



February, 2012

## **TABLE OF CONTENTS**

SECTION 1 - THE DISASTER READINESS TEAM .....	4
1.1    PURPOSE .....	4
1.2    ORGANIZATION AND PLANNING .....	4
1.3    EMERGENCY COORDINATOR .....	5
1.4    ALTERNATE EMERGENCY COORDINATOR.....	6
1.5    THE USE OF EMERGENCY ACTION TEAMS .....	6
1.6    EMERGENCY CONTROL CENTER.....	7
SECTION 2 – CRITICAL APPLICATIONS .....	8
2.1    CRITICAL SYSTEMS AND APPLICATIONS .....	8
2.1.1    DISASTER/RECOVERY PLANNING VS. BUSINESS CONTINUITY PLAN.....	8
2.1.2    OVERARCHING DISASTER/RECOVERY STRATEGY .....	8
2.1.3    ESTABLISHING A PRIORITY FOR RECOVERY FROM A DISASTER EVENT .....	9
2.1.4    CRITICAL SYSTEMS AND APPLICATIONS .....	10
2.1.4.1    CRITICAL SYSTEMS (A THROUGH G) .....	10
2.1.4.2    CRITICAL APPLICATIONS (A1 THROUGH G3).....	12
2.2    RECOVERY METHODOLOGY .....	19
2.2.1    INTRODUCTION AND ASSUMPTIONS .....	19
2.2.2    NETWORK SERVICES.....	19
2.2.3    "CONSTANT" OR "ALWAYS ON" SERVICES - NO FAILOVER OR INTERVENTION REQUIRED .....	20
2.2.4    "NON AUTOMATED FAILOVER" SERVICES .....	20
SECTION 3 - GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS .....	21
3.1    FIRES, FLOODS AND ELECTRICAL OUTAGES .....	21
3.1.1    CONTINGENCY PLANS AND PROCEDURES .....	22
3.2    HARDWARE FAILURES .....	24
SECTION 4 - REDUCING RISKS .....	25
4.1    PROTECTION OF COMPUTER DATA .....	25
4.1.1    BACKUP PROCEDURES .....	25
4.1.2    OFFSITE BACKUP RECOVERY PROCEDURES .....	26
4.2    PROTECTION OF THE UNC-GA COMPUTER ROOM .....	26
4.2.1    PHYSICAL SECURITY .....	26
4.2.2    ACCESS SECURITY.....	27
4.3    BACKUP OF DATA, HARDWARE, SUPPLIES & DOCUMENTATION.....	27
4.4    INSURANCE.....	28
SECTION 5 – UNC-GA "HOT-SITE"/CONTINGENCY SITE DESCRIPTION.....	28
5.1    UNC-GA HOT-SITE.....	28
SECTION 6 - RECOVERY PROCEDURES FOR A MAJOR DISASTER.....	29
6.1    EMERGENCY ACTION TEAMS AND RESPONSIBILITIES.....	29
6.1.1    APPLICATIONS TEAM.....	31
6.1.2    NETWORK & COMMUNICATIONS TEAM .....	31
6.1.3    FACILITIES TEAM.....	32
6.1.4    ADMINISTRATIVE TEAM.....	33
6.1.5    SYSTEMS TEAM.....	34
6.2    NOTIFICATION OF THE READINESS TEAM.....	35
6.3    INITIAL READINESS TEAM PROCEDURES .....	36
6.4    ACTIVATION OF THE EMERGENCY CONTROL CENTER .....	36
6.5    NOTIFICATION OF EMERGENCY ACTION TEAMS AND TOP MANAGEMENT.....	37
6.6    NOTIFICATION OF OFFSITE STORAGE AND CONTINGENCY SITES.....	38
6.7    SUMMARY OF PROCEDURES FOR CONTINGENCY OPERATIONS .....	38
6.8    PROCEDURES FOR REPLACEMENT OF COMPUTER ROOM.....	39
6.9    PROCEDURES FOR RETURN TO NORMAL OPERATIONS .....	40
SECTION 7 - TESTING AND MAINTENANCE OF THE PLAN.....	41
7.1    PROCEDURES FOR TESTING .....	41

7.2	PROCEDURES FOR REVIEW AND UPDATE .....	42
7.3	CRITICAL SYSTEMS TEST PLAN (SEE SECTION 2 FOR CRITICAL SYSTEMS AND APPLICATIONS) .....	43
7.3.1	CRITICAL SYSTEMS TEST PLAN HISTORY .....	44
	The Emergency Coordinator will keep a wiki (wiki.northcarolina.edu) that will log each execution of the critical systems test plan outlined above. This wiki will describe the test performed as well as its outcome. The CIO will review and approve the log every 6 months (July 1 and Jan 1). .....	44
7.4	RECOVERY TEST PLAN .....	44
7.4.1	LATEST RECOVERY TEST .....	44
7.5	Signatures .....	45
7.6	Revisions .....	46
	SECTION 8 - APPENDICES .....	47

# **SECTION 1 - THE DISASTER READINESS TEAM**

## **1.1 PURPOSE**

The purpose of the Readiness Team is to establish and direct plans of action to be followed during an interruption of computer services caused by a disaster or other lesser emergency. As the name implies, the Readiness Team maintains readiness for emergencies by means of the **DISASTER RECOVERY PLAN**. The Readiness Team is also responsible for managing the disaster recovery activities following a disaster, and can be thought of as the "disaster management team." Through the disaster plans, the Readiness Team will provide for:

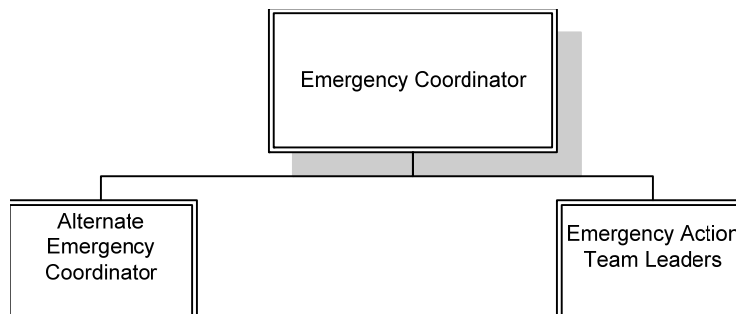
- The safety of personnel
- The protection of property
- The continuation of UNC-GA Information Resources (UNC-GA IR) functions

## **1.2 ORGANIZATION AND PLANNING**

The Readiness Team consists of an Emergency Coordinator, an Alternate Emergency Coordinator, the Action Team Leaders, and any other designated individuals. The list of designated members of the Readiness Team, showing names and functions, is provided in:

*See Appendix E.1 - Emergency Notification List (Readiness Team).*

### **THE READINESS TEAM**



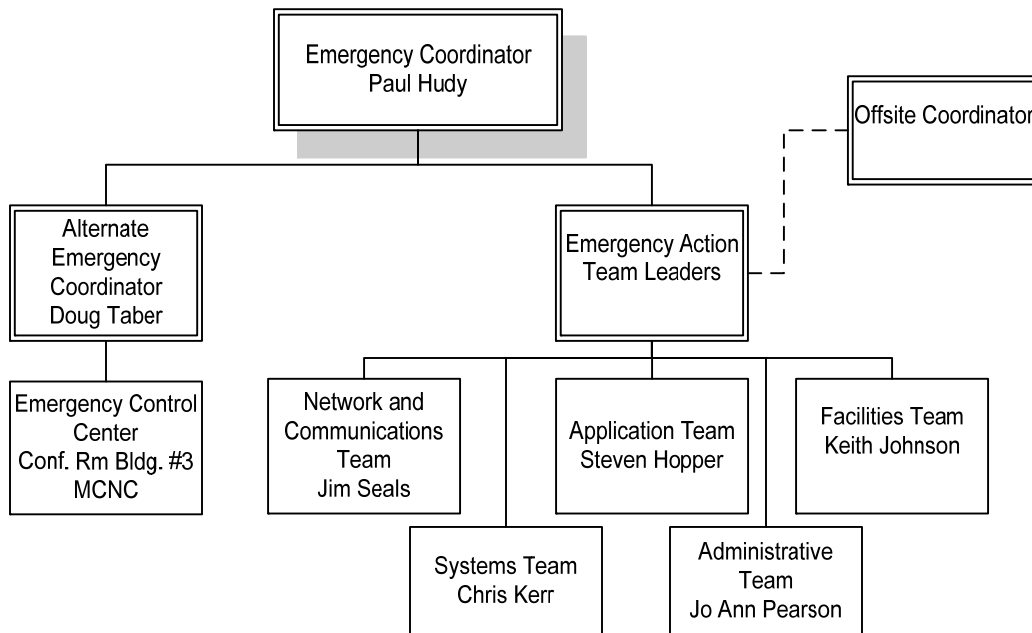
The responsibilities of individuals assigned to the Readiness Team are in addition to their regular assignments and are made on the basis of familiarity and competence in their respected areas or specialties.

The D/R Plan is administered by the Emergency Coordinator and the Alternate Emergency Coordinator. The Alternate Coordinator is also responsible for maintaining an Emergency

Control Center. Emergency Action Teams are used to facilitate the response to various types of emergency situations.

The responsibilities of the Coordinators, the functions of Emergency Action Teams and team leaders, and the purpose of the Emergency Control Center are defined later in this document (Section #6). The overall organization for the management of emergencies is illustrated by the following diagram.

### ORGANIZATION FOR EMERGENCIES



### 1.3 EMERGENCY COORDINATOR

The Emergency Coordinator is responsible for developing and coordinating the Readiness Team. During an emergency situation, the Emergency Coordinator will activate and then direct all activities until the emergency is under control. In the absence of the Coordinator, the Alternate Emergency Coordinator will assume his/her duties. Additionally, the Coordinator is responsible for the following:

- Reviewing, evaluating, and updating the **Disaster Recovery Plan** at least annually to assure that all emergency situations have been adequately considered and that appropriate contingency plans have been prepared.
- Ensuring that the emergency teams and other employees receive proper training of emergency plans and procedures. This will routinely be done as a part of periodic tests of

the disaster plan. The Coordinator will also ensure that new employees are properly trained and that certain emergency procedures are reviewed as frequently as necessary.

- Conducting meetings with the Alternate Coordinator, the Offsite Coordinator (MCNC “Hot-site” contact), and the Emergency Action Teams as necessary.
- Keeping all members of the Readiness Team fully briefed on all aspects of the disaster plan.
- Evaluating the readiness and proficiency of each Emergency Action Team and the appropriateness of their assignments.
- Keeping management informed of the status of the Readiness Team and the Disaster Recovery Plan.
- Communicating the status of emergency situations to management promptly and efficiently.
- Maintaining liaison with local agencies, other company locations, and other involved parties as appropriate.

The designated Emergency Coordinator is identified in:

*Appendix E.1 - Readiness Team and Emergency Notification List.*

## 1.4 ALTERNATE EMERGENCY COORDINATOR

In the absence of the Emergency Coordinator, his duties will be assumed by the Alternate Emergency Coordinator. The following additional duties are assigned to the Alternate Coordinator:

- Assisting the Emergency Coordinator in maintaining an up-to-date **Disaster Recovery Plan** and other emergency procedures, and in directing proper distribution of the plans.
- Providing emergency evacuation programs and posting them on bulletin boards or otherwise distributing them to all personnel.
- Maintaining up-to-date listings of Offsite Emergency Coordinators, Emergency Action Team members, and emergency telephone numbers.
- Activating the Emergency Control Center and administering the Control Center itself during an emergency situation.
- Keeping the Emergency Control Center properly equipped and in a state of readiness.
- Monitoring all tests of the **Disaster Recovery Plan**, and recording the progress, problems, and successes.

The designated Alternate Emergency Coordinator is identified in:

*Appendix E.1 - Readiness Team and Emergency Notification List*

## 1.5 THE USE OF EMERGENCY ACTION TEAMS

Emergency Action Teams are used for specific functions during an emergency situation and subsequent recovery. The teams and their responsibilities are defined in **Section 6**.

Designated leaders are identified in:

*Appendix E.1 - Readiness Team and Emergency Notification List*

In general, the Team Leader of each team is responsible for the following duties:

- Periodically reviewing and evaluating the emergency planning with particular emphasis on completeness and accuracy of specific recovery procedures, team responsibilities, assignments of and changes in personnel, and availability of equipment, facilities, and services.
- Recommending to the Emergency Coordinator any necessary changes or improvements in the Plan.
- Recruiting and training personnel for emergencies and maintaining proficiency at a high level. All team members must be capable of performing their duties quickly under stress.
- Informing the Emergency Coordinator of any additions or changes of individuals assigned to the Action Team.

## **1.6 EMERGENCY CONTROL CENTER**

In the event of a major disaster, the Emergency Control Center (ECC) will be activated and the ECC will direct all communications and activities. The Control Center will be used to coordinate the management of recovery procedures, and will serve as the center of all communications between the Emergency Coordinators, the Action Teams, and all other personnel.

The administration of the Control Center is the responsibility of the Alternate Emergency Coordinator. UNC-GA IR has an office presence in building #3 on the MCNC campus at RTP, NC ( see section 5.1).The building is physically located over five miles away from the UNC-GA main facility. Due to the comprehensive information technology infrastructure and network connectivity already available in these offices, the Disaster Readiness Team will use the MCNC facility as the primary ECC.

- The designated Emergency Control Center and alternate locations are identified in **Section 6.4**.
- The Emergency Control Center will be activated when a major disaster has occurred, especially when the personal safety of employees or property is jeopardized. Readiness and activation of the Control Center are the responsibility of the Alternate Coordinator. Direction of activities and communications from the Control Center is the responsibility of the Emergency Coordinator.
- This center will provide centralized and coordinated control of communications during emergencies. When the Emergency Control Center is in operation, Emergency Coordinators and Action Team Leaders will coordinate with the center and keep it informed of status and progress. If conditions warrant closing of facilities, the Emergency Control Center will communicate the closing notice through the management chain to all employees.

## **SECTION 2 – CRITICAL APPLICATIONS**

### **2.1 CRITICAL SYSTEMS AND APPLICATIONS**

UNC-GA Information Technology (IT) provides several critical systems to service the business and academic needs of the UNC System and its constituent institutions. To ease the effort to define a disaster/recovery plan, the primary systems have been grouped into seven major categories, with each of these major categories comprised of several individual applications. The seven major systems categories are: Network Services, VM Ware, UNC Online, Ancillary Applications, Institutional Research and Analysis, Database Environment, and Security and Identity Management (See Appendix F).

These major systems groupings have been created to recognize the similarities of the IT infrastructure environment required for successful operation of the related applications and, also, to allow for the definition of a priority schema of sequential recovery of the systems, if a priority must be set.

#### **2.1.1 DISASTER/RECOVERY PLANNING VS. BUSINESS CONTINUITY PLAN**

To understand the purpose of this plan, another important item is the delineation between disaster/recovery and business continuity. The procedures and practices defined in this plan ensure that the IT critical systems are restored to operation in a rapid response to a disaster event that destroys partially or completely the primary IR operations housed in the data processing center of the Spangler Building at 910 Raleigh Rd. Chapel Hill, NC. The plan does not address the notification of all of the UNC-GA staff that a disaster has occurred and it does not offer procedures for the staff to resume operations in some other location.

One basic assumption of this D/R plan is that, in the event of an emergency, UNC-GA staff must have Internet connectivity to access the backup recovery site. As long as an individual can access the network services provided by the Internet, the automated systems and services provided by UNC-GA will be available.

#### **2.1.2 OVERARCHING DISASTER/RECOVERY STRATEGY**

It is important to note that this D/R plan attempts to classify and categorize the many systems supported by UNC-GA for the purpose of offering a tiered approach to the restoration of IT services in the event of a disaster. In reality, the actions in response to a disaster will be holistic and all systems will be restored in a brief period of time in a set order. The restoration of the systems operation will be done simultaneously which will be transparent to our user community as it will appear to be a simultaneous restoration and not a step by step approach.



UNC-GA IR has a true “hot-site” environment installed in the backup site at MCNC and, upon becoming aware of a disaster, critical IT services will be restored to an operational state in under four hours. This rapid fail-over has been successfully tested and will continue to be tested at least twice a year.

It is also important to note that D/R is an all or nothing strategy and there does not need to be a partial recovery of anything. All critical applications will be restored intact and there are no special forms, equipment, or networking gear necessary for any subset of UNC-GA applications. In addition, there is no attempt to identify or define alternative manual systems that can be invoked in the wake of a disaster event as they would be irrelevant.

### **2.1.3 ESTABLISHING A PRIORITY FOR RECOVERY FROM A DISASTER EVENT**

As stated above, in one sense it is not necessary to establish a priority for the reintroduction of the critical applications in the event of a disaster as all applications will be restored in a unified manner. Although the many applications supported by UNC-GA IR will all be restored in a concurrent manner, there is need to assign a priority tier so that we will have a method to determine who should be contacted to verify that the application is, in fact, operating correctly in the restored mode.

If a disaster does occur, UNC-GA IR will, first, restore all of the critical systems and, then, will notify either the primary or secondary user contact to verify that the restored application is functioning correctly. The priority tiers are:

- Tier A – the system is fundamental to the operation of all other systems and must be working correctly prior to any other system being verified. An example of a Tier A assignment is the “Active/Directory” application which must be functional to authenticate a user for access to other UNC-GA applications.
- Tier B – an important daily business operation is dependent upon the application being available. An example is the “Inter-institutional Registration (IIR)” application as the ability of students to register for online courses is completely dependent upon the successful operation of UNC Online IIR.
- Tier C – the application is not required for a daily business operation. Business operations can run successfully for an extended period without the application being available. This tier includes applications such as the Lime Survey data collection tool.

Integral to the assignment of an application to a tier is the length of outage that can be tolerated. Hence, related to a tier assignment is the definition as to how long a system outage may be tolerated. The following periods apply:

- Tier A – no tolerance, the application must be restored immediately (less than 4 hours)
- Tier B – some tolerance, the application may be out of service for 1 business day and up to 3 business days in case of a serious catastrophe. It is important to restore the application quickly but, in the event of a disaster, a full day (or more) outage can be tolerated.
- Tier C – significant tolerance, the application may be out of service for 3 business days or greater without a serious impact on the daily business operations of UNC-GA or any of its constituent institutions.

It is important to state that the Tier assignments are meaningful only in the time that will be allowed for the primary or secondary contact person to verify that their application has been restarted correctly. Once the “hot-site” is activated, it is important to verify that the every individual application is operating correctly. The primary or secondary contact must connect to their application and test the functionality to ensure it has been restored correctly.

In the case of a disaster event, there may be a chaotic work environment and many individuals will have several responsibilities related to restoring applications. The Tier assignment of each system gives the primary and secondary contact guidance regarding the relative importance of the D/R testing which is expected to be performed. A Tier “A” assignment requires an immediate response and a Tier “C” assignment would require a more relaxed response for the application verification testing.

## 2.1.4 CRITICAL SYSTEMS AND APPLICATIONS

### 2.1.4.1 CRITICAL SYSTEMS (A THROUGH G)

	<b>Critical Systems</b>	<b>Systems Description</b>	<b>Standard Operational Hardware</b>	<b>Required D/R Hardware</b>
<b>A</b>	<b><i>Network Services</i></b>	<ul style="list-style-type: none"> <li>• This category of applications includes the basic network address issuance and recognition for Internet access to the UNC-GA information technology services.</li> </ul>	Infinity Kazran	Eternity Sardick
<b>B</b>	<b><i>VMware</i></b>	<ul style="list-style-type: none"> <li>• Standard suite of software systems to support the business offices and staffs of UNC-GA. The systems are comprised of the typical utility systems such as electronic mail (e-Mail), calendaring and scheduling, the static website containing general information concerning UNC, the central document repository for common reports,</li> </ul>	UNCGACS4 UNCGACS5 UNCGACS6 UNCGACS7 UNCGACS8 UNCGACS9 (Dell R710) AESIR EQ Group	UNCGAHS1 UNCGAHS2 UNCGAHS3 VANIR EQ Group (SAN)

	<b>Critical Systems</b>	<b>Systems Description</b>	<b>Standard Operational Hardware</b>	<b>Required D/R Hardware</b>
		and a series of systems that collect, store, and report on information related to academic and business needs		
<b>C</b>	<b><i>UNC Online</i></b>	<ul style="list-style-type: none"> <li>A series of systems allowing distance education students to investigate the availability of online academic programs, register in courses, reserve time with exam proctors, and other related services. It is an important asset to UNC Online for daily business operations.</li> </ul>	TUNCOLB1, TUNCOLB2, TUCNCO 1, TUNCO 2, TUNCO 3, Oracle02, TUNCODB1, and TUNCODB2 Oracle04(DB), Torchwood(DB)	TUNCOLB2 Oracle05(DB) Pandorica(DB)
<b>D</b>	<b><i>Ancillary Applications</i></b>	<ul style="list-style-type: none"> <li>A small group of applications that do not have a home in any other category. These ancillary applications include Database software (Filemaker Pro) for use by IR application development staff and some end user developers.</li> <li>CommVault Laptop Backups</li> </ul>	FileMaker Dalek OpServer	N/A
<b>E</b>	<b><i>Institutional Research and Analysis</i></b>	<ul style="list-style-type: none"> <li>UNC-GA IR hosts an entire suite of data collection and reporting systems for the Institutional Research and Analysis Division of UNC-GA. As a host, IR does not develop nor maintain the software application but serves solely as a custodial partner to operate, backup, restore, and manage access.</li> </ul>	Barney (Dell 2950)	Hot Barney (Dell 2950)
<b>F</b>	<b><i>Database Environment</i></b>	IR has two primary relational database software applications for the development and operation of its IT application. Oracle and MySQL are the database tools that are used for UNC-GA systems applications.	Torchwood Oracle 04 Gridcontrol	Pandorica Oracle 05
<b>G</b>	<b><i>Security and Identity</i></b>	End user authentication and	Pangol; see vmware environ	Fendahl; see vmware

<b>Critical Systems</b>	<b>Systems Description</b>	<b>Standard Operational Hardware</b>	<b>Required D/R Hardware</b>
<i>Management</i>	authorization is a basic infrastructure need to ensure privacy and security of UNC-UNC-GA technology services and database resources. This suite of applications is the central core of security services to limit access to licensed users and ensure appropriate utilization of the available IT systems applications.	skaro	environ.

#### 2.1.4.2 CRITICAL APPLICATIONS (A1 THROUGH G3)

	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
<i>A1</i>	<i>Network Services</i>	Dynamic Host Control Protocol (DHCP)	Service that provisions the IP address space to user workstations and devices	D. Taber C. Kerr	<b>A</b>	550
<i>A2</i>		Domain Name Services (DNS)	Service that resolves names to IP addresses for the machines within the northcarolina.edu domain, etc	D. Taber C. Kerr	<b>A</b>	unlimited
<i>A3</i>		Network Time Protocol (NTP)	Service that provides the reference clock to enable the synchronizing of systems and servers	D. Taber C. Kerr	<b>A</b>	all servers
<i>B1</i>	<i>VMware</i>	e-Mail	Primary mode of staff to staff communication. Very important to daily business operation for any organization.	D. Taber C. Kerr	<b>A</b>	550 /550
<i>B2</i>		Clustered Web Services	Provide a load-balanced HA Apache Environment	D. Taber C. Kerr	<b>B</b>	300,000+
<i>B3</i>		ActiveCollab	Systems utility to collect and store documents in a central shared repository. Allows several individuals to work on	L. Connolly P. Hudy	<b>B</b>	1000 /4000

	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
			the same series of documents without the need to duplicate for each team member.			
<b>B4</b>		Lime Survey	User friendly survey tool allowing for ease of setup and completion of typical survey events. It is open source software that has been modified to allow access using Federated ID Management for a semblance of privacy and security for sensitive data collection.	L. Razack S. Hopper	<b>C</b>	1000/10
<b>B5</b>		College Preparatory Data Management System	Web application with the functionality to enter student and professional development activity, request and import national survey data, and display, print, and export reports.	C. Tillery	<b>B</b>	200/30
<b>B6</b>		Suspension and Expulsion	This application provides a clearinghouse for suspended and expelled students and the ability to insure university applicants are not on the list.	K. Dixon S. Hopper	<b>B</b>	50/5
<b>B7</b>		Facilities Management	Provides data management for utilization of buildings and rooms of an institution. Data is entered for hourly usage of building rooms and reports are available.  PRIMARY USERS: UNC-GA, University of North Carolina campuses, North Carolina Community Colleges, and private educational institutions.	J. Hill/Allen Lakomiak	<b>C</b>	300/100
<b>B8</b>		NC Quest	This application is used to support federal grants. Data is uploaded and displayed for review. The Division of	Alisa Chapman\Cody Thompson	<b>C</b>	30/20

	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
			<p>University-School Programs and the UNC Center for School Leadership Development, and in partnership with the NC Department of Public Instruction, is issuing this request for proposals, entitled NC QUEST (North Carolina Quality Educators through Staff Development and Training).</p> <p>PRIMARY USERS: UNC-GA Academic Affairs and Center for School Leadership and Development.</p>			
<b>B9</b>		CAPSTAT	<p>UNC's Capital Project Status System. Provides data entry of budget and draw information by contractor and reporting for capital projects related to the University of North Carolina.</p> <p>PRIMARY USERS: UNC-GA and campuses.</p>	Miriam Tripp / Allen Lakomiak	<b>C</b>	50/18
<b>B10</b>		Expansion Budget	<p>Web portal for UNC system campuses to enter annual continuation budget information for the fiscal year. This application accepts projected enrollment from the campuses and is used to aggregate and prioritize the data for the North Carolina odd year budget cycle.</p> <p>PRIMARY USERS: UNC-GA Finance Division and university staff.</p>	Ginger Burks /Angelisa Riggsbee	<b>C</b>	25/18
<b>B11</b>		Enrollment Management	<p>Provides for the entry of projected full time equivalent students and head counts by institution for a given year and reports required to request financial support from the North Carolina State</p>	G. Burk/ A. Lakomiak	<b>C</b>	100/18

	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
			Legislature.  PRIMARY USERS: UNC-GA Finance and Academic Affairs Divisions and University of North Carolina campuses.			
<b>B12</b>		Human Resources Positions and Personnel	“The Hopper” tracks personnel, hiring and termination data which feed the Performance Management System. This application is used to define positions and enter and maintain information related to persons associated with these positions.  PRIMARY USERS: UNC-GA Human Resources Division, Division Managers, UNC TV managers, and SEAA managers.	R. Snuggs/ D. Davis	<b>B</b>	550/15
<b>B13</b>		Performance Evaluations	Performance Management System approved by the Office of State Personnel. This application provides the functionality for the manager to create employee work plans and evaluate employee performance against these plans.  PRIMARY USERS: UNC-GA, UNC TV, and SEAA employees.	G. Davis D. Davis	<b>B</b>	550/250
<b>B14</b>		Orientation	Online orientation system for newly hired employees at the University of North Carolina General Administration and the campuses to acquaint them with the history and mission of their organization. In addition, it provides information on programs and services, payroll	D. Watts A. Lakomiak	<b>B</b>	Unlimited /550

	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
			and leave policies, and benefits.  PRIMARY USERS: New hires of UNC-GA, UNC TV, and SEAA.			
<b>B15</b>		Staff Assembly	A content management site for UNC system Staff Assembly documentation. The assembly includes representatives from UNC-GA and all other campuses within the UNC System. The application serves as a repository for meeting minutes, agendas, schedules, and other content relevant to the activities of the Staff Assembly.	Debbie Robertson Ann Lemmon	<b>C</b>	Unlimited/ 30
<b>B16</b>		Optional Retirement Plan(under development)	Privatized version of the State Retirement System optionally available to all EPA employees within the UNC system	Diane Watts Brian Usischon	<b>C</b>	Unlimited/ 18
<b>B17</b>		UNC Federation (Shibboleth)	Single-sign-on interface across UNC system. Allows for inter-campus coordination and authentication of end users.	Steven Hopper	<b>A</b>	Unlimited/ Unlimited
<b>B18</b>		Web Services	Back-end server to server components that support UNC-GA web applications. This application is required for the successful operation of all of the UNC Online applications of inter-institutional services.	Steven Hopper	<b>B</b>	Unlimited/ Unlimited
<b>B19</b>		UNC Online	UNC system online portal that consist of public facing online catalog of course offerings and inward facing academic services portal consisting of	Steven Hopper	<b>B</b>	Unlimited/ Unlimited



	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
			registration system and exam proctoring.			
<b>B20</b>		Website	UNC-GA web presence to support all of the central office services as well as the Board of Governors.	Kathy Jones Alex MacKethan	<b>B</b>	Unlimited/ Unlimited
<b>C1</b>	<b>UNC Online</b>	Primary Website	Main UNC Online web presence, which provides information related to all procedures, practices, events related to distance education.	Steven Hopper	<b>B</b>	Unlimited / Unlimited
<b>C2</b>		Inter Institutional Registration System	Provides the ability for a student at a UNC institution to enroll in a course at another UNC institution.	Steven Hopper	<b>B</b>	200,000 / 100
<b>C3</b>		Exam Proctoring	Administers the proctoring of exams for UNC Distance Education courses. This includes the recruiting and licensing of proctors, the provision of exams by faculty, the scheduling of proctored exams by students with guidance from the proctor.	Amanda Dough Steven Hopper	<b>B</b>	20,000 / 1,000
<b>C4</b>		Electronic Mentoring	Allows academic programs across the UNC system the ability to create and manage a pool of mentors and match their students with these mentors. The current customer is NCSU's Professional Science Master's program.	Lisbeth Borbye Steven Hopper	<b>B</b>	1,000/100
<b>D1</b>	<b>Ancillary Applications</b>	Filemaker Pro	Application for reporting and storing data. Used for Network Services inventory of hardware, software, and licenses. Law department uses to track complaints. HR uses to track Optional Retirement	Diane Watts Paul Hudy	<b>C</b>	25/5

	<b>Critical Systems</b>	<b>Critical Applications</b>	<b>Application Description</b>	<b>Primary / Secondary Contact</b>	<b>Priority Tier</b>	<b>Number of Users Max / Concur.</b>
			recipients.			
<b>E1</b>	<b><i>Institutional Research and Analysis</i></b>	DIRS Website / Data Upload and Report repository	Two servers that house institutional data to serve as the basis for all IR research and analysis for UNC-GA. FTP server and Static HTML pages provide an interface for report consumption.	Dan Cohen-Vogel Sofia Kwon	<b>B</b>	100 / 20
<b>F 1</b>	<b><i>Database Environment</i></b>	Oracle	Oracle 11g database environment to house the data for our online production applications.	Allen Lakomiak Chris Stefanick	<b>A</b>	Unlimited / Unlimited
<b>F2</b>		MySQL	Database back-end to various applications with the UNC-UNC-GA environment	D. Taber A. Lakomiak	<b>A</b>	Unlimited / Unlimited
<b>G1</b>	<b><i>Security and Identity Management</i></b>	Active Directory /LDAP	Services that provides the login/password provisions the users accounts, authorization and authentication polices to the users and workstations operating within the northcarolina.edu domain	D. Taber C. Kerr	<b>A</b>	550/550
<b>G2</b>		UNC Federation and Shibboleth	Service that provides the authentication mechanism for “shibbolized” applications accessed by UNC-GA and UNC Campuses; Part of the UNC Federation; Services operate as both an Identity Provider (UNC-GA only) and Identity Service Provider (UNC system)	S. Hopper/D. Taber	<b>A</b>	200,000 / 1000
<b>G3</b>		Radius	Service that provides centralized Authentication, Authorization, and Accounting ( <a href="#">AAA</a> ) management for guest access to UNC-GA public network; not available at hot-site so no DR plan	D. Taber K. Johnson	<b>B</b>	50/50

## **2.2 RECOVERY METHODOLOGY**

### **2.2.1 INTRODUCTION AND ASSUMPTIONS**

This D/R plan and recovery procedure addresses the failure or destruction of the computer room and the installed server and networking components located at 910 Raleigh Road in the Meredith Spangler building. The plan's scope assumes the "worst case" total destruction or failure of the machine room and how it would impact IT infrastructure and centralized services that require that infrastructure to operate. The restoration of these services is assumed to occur at the "hot-site" IT infrastructure which is maintained by UNC-GA IT technical staff and which is located at MCNC, Building 3, in Research Triangle Park, North Carolina.

The plan's scope does not address the ability of any individual UNC-GA staff member to work from a particular location or machine once those services are restored. If a staff member has Internet connectivity, she/he will be able to access the recovered services in operation at the MCNC "hot-site".

When this recovery plan is enacted, UNC-GA centralized IT services will be available and operating for any user who can reach the internet. The plan does not assume that user will be located at UNC-GA or UNC CSLD as any physical destruction of the machine room may also impact the fiber cable plant and telecommunication closet networking infrastructure that serves those two buildings.

This recovery plan also assumes that all UNC-GA networking and systems personnel are available to respond to the crisis. If personnel availability is impacted, this could extend the time of recovery or prohibit it entirely beyond the short or medium time frame [see risk assessment].

Finally, the plan assumes the operational status and access to the MCNC facilities has not been impacted by whatever disaster has impacted the primary UNC-GA operating facilities.

### **2.2.2 NETWORK SERVICES**

As access to the Internet is essential for the enactment of this plan, the 152.4.x.x network must be made available at the MCNC hot-site before most of the below services will be functional (see Appendix A for Communications Recovery Diagram). Estimated time to completion under working assumptions is approximately 1 to 2 hours (Persons responsible: Keith Johnson, Jim Seals).

1. The router installed at MCNC will advertise parts of our class B address space from our MCNC hot-site racks. The address space that will be advertised is 152.4/18.
2. Routes will not be advertised until UNC-GA goes down; switch-over is automatic
3. SSH via the router will allow management access into the firewall.
4. Firewall, ASA5510, installed behind the router will provide security options and ipsec tunnels for payroll services
5. Firewall interface facing MCNC is configured as 'OFF' to eliminate duplicate gateway IP address problems

6. When the primary site at UNC-GA goes down, the hot-site router will start advertising UNC-GA's address space. Once the advertising is initiated, SSH via the router will allow access to the firewall's management interface to enable the inside interface of the firewall. Since the hot-site ASA has the same outside interface address as the Banner VPN box at UNC-GA, the tunnels to the campuses will re-establish themselves automatically. [Routing and tunnel connections will be tested in February, 2012]

### **2.2.3 "CONSTANT" OR "ALWAYS ON" SERVICES - NO FAILOVER OR INTERVENTION REQUIRED**

The following set of services is "always on" and will continue to operate without additional manual intervention regardless of the state of the GA building facilities. .

1. Secondary DNS (Does not require 152.4.x.x network)
2. Secondary Mail Gateway (Does not require 152.4.x.x network)
3. AD authentication
4. AD Filestore
5. VMware (Hot-site services only)
6. VMware View
7. MS Exchange 2007 (dependent on state of "token" passing)
8. Websites ( Hot Site Services only: Sardick 1/3<sup>rd</sup> of Vhosts, PEG)

### **2.2.4 "NON AUTOMATED FAILOVER" SERVICES**

These services will require some level of human interaction. The basic requirements are listed. Estimated time to completion under working assumptions is 1 to 2 hours. (Persons responsible: Doug Taber, Chris Kerr, Obie Deyo)

1. VMware - Main site services (Prerequisites: 2.2.2-1, 2.2.3-5) To bring main site virtual machines online:
  - a. The replica sets on vanir SAN must be promoted to Volumes
  - b. The iSCSI Volumes must be mapped on the VMware Hosts
  - c. The Virtual servers must be registered in VMware
  - d. Prioritize servers to come up based on needs.
2. Primary DNS (Prerequisites: 2.2.-1,) This will be restored upon completion of VMware Main-site restoration
3. Primary Mail Gateway ((Prerequisites: 2.2.2-1, 2.2.4-1, 2.2.4-2) This will be restored upon completion of VMware Main-site restoration
4. Terminal Services (Prerequisites: 2.2.2-1,2.2.4-1, 2.2.4-2) This will be restored upon completion of VMware Main-site restoration
5. Fred/Barney (Prerequisites: 2.2.2-1)
  - a. Routing rules will need to be updated
  - b. Firewall rules will need to be updated
  - c. Replicates to "Betty" aka "Hot Barney"

6. Ethel (Prerequisites: 2.2.2-1) available via VMWare view environment – see#1
7. FileMaker 5.5 (Prerequisites: 2.2.2-1, 2.2.4-2) This will be restored upon completion of VMWare Main-site restoration
8. FileMaker 11.0 (Prerequisites: 2.2.2-1, 2.2.4-2) This will be restored upon completion of VMWare Main-site restoration
9. Oracle grid controller will switch over to hotsite (check with A. Lakomiak)
10. MySQL Server As part of normal daily operations, MySQL server data is replicated to the hot-site within minutes of writing to the production system. Re-establishment of the production at the hot-site will involve repointing of services to the hot-site MySQL box. (servers: "torch wood (master) "/"pandorica" (slave))
11. Subversion See #10 above
12. MS Exchange 2007 will be restored upon VM restoration

## **SECTION 3 - GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS**

A series of procedures follow as a reference for prompt and appropriate actions to be taken in potential emergencies or events which cause interruption of computer service.

Orientation sessions are to be held periodically to familiarize UNC General Administration Information Resources [UNC-GA-IR] employees with these procedures and to outline responsibilities in the event of such emergencies. The Emergency Coordinator will arrange these training sessions.

Copies of this Plan are to be kept in key locations for ready reference. A copy of this plan will also be kept on the UNC-GA IR website. Members of the Readiness team are to be given copies of this plan at home and/or at work.

The assets of the UNC System are extremely important to its operation. The most important asset is our personnel. Risks should not be taken to save other assets where personnel may be in jeopardy.

### **3.1 FIRES, FLOODS AND ELECTRICAL OUTAGES**

### 3.1.1 CONTINGENCY PLANS AND PROCEDURES

#### a. PREVENTION

Periodically review all areas of Information Resources [IR] responsibility for evidence of potential leaks, flooding, or combustible materials. Areas beneath raised floor panels and above ceiling tiles should also be inspected as appropriate. Floor panel lifters are located in the computer room and operations area [Computer Room - Spangler Center, 1st Floor Annex, Room 317.]

Operational areas of Information Resources should be sight checked periodically by the IR staff.

All new IR employees will be educated about procedures relating to flood, fire or electrical outages. IR employees will have periodic reviews of the plan on a schedule to be determined by the Emergency Coordinator.

Regular site inspections which include general area review and checks of electrical connections are made by UNC Chapel Hill Physical Plant. Fire extinguishers are checked on a routine basis by the UNC Chapel Hill Physical Plant Office of Environmental Health and Safety. Inspections of the computer room fire and HALON systems are performed every six months by BFPE International.

#### b. DETECTION

##### 1. FIRE

**If the fire is such that employees must evacuate the building, call 911** and give them the **building address and the location** (Room Number) of the fire within the building. If fire alarms are sounding, then the building alarm system will have already signaled to the Campus Police. Computer Room (Rm. 317)

The computer room has a fire detection and HALON fire suppression system. Inspections of these systems are performed every six months by BFPE International. If smoke is detected, horns will sound inside the computer room. A zone detection panel is located in the Computer Room, Room 317 and indicates which detectors are in alarm condition. The detection system is connected to the building alarm system which will automatically send the alarm to the UNC Chapel Hill Campus Police who are responsible for notifying the local fire department. **DO NOT ENTER THE ROOM IF THE FIRE ALARM IS SOUNDING.**

#### **Extinguishing Fires Outside of the Computer Room**

The staff will be trained in the use of fire extinguishers during the periodic fire plan reviews. A single extinguisher is located in the 1st Floor Annex Stairwell (north end). A second fire extinguisher is located in the paper storage room (Rm. 316) adjacent to the UNC-GA computer room. Employees should only attempt to extinguish a fire if it is very small or confined to a particular piece of equipment. Otherwise, the fire department should be called and the building should be evacuated immediately.

## 2. FLOODING

The risk of naturally occurring flooding at the Spangler Center is highly unlikely without a prior closing of the facility due to an adverse weather event. If such event should occur, the employees should follow established evacuation routes. If a man-made leak or flooding is detected, the employee should immediately call UNC Chapel Hill Physical Plant. (919) 962-3456. The IR staff should be notified to assess risk to any information technology resources.

## 3. ELECTRICAL OUTAGES

In the case of local and regional electrical outages, the computer room (Rm. 317) will automatically switch to UPS power and then to generator power. The computer room will return to local “line” power once the system detects that power has been restored and has been stable for a period of time. The generator is powered by a natural gas pipeline, thus the computer room can operate in “generator mode” for an indefinite period of time.

The general building is not powered by any alternative power source and will lose electrical power during regional or local power interruptions. There will be limited auxiliary lighting during such an event. Employees should use care when exiting the building and follow the established evacuation plan. UNC Chapel Hill Physical Plant should be notified of any power outages. (919) 962-3456

### c. BUILDING EVACUATION

If the emergency rises to the level that requires evacuation of the building, please follow established evacuation routes. (See Appendix D Building Evacuation Floor Plan)

When leaving the building, exit by using the stairs. Do not use the elevator. If fire blocks the designated escape route, please find an alternative escape route or, if necessary, exit the building through an office window

#### Evacuation Plan for Information Resources Division

In cases of fire or other life threatening emergency, the IR division staff should immediately evacuate the building via the closest available exit. The IR staff occupies the first floor offices of the Spangler Annex; specifically Rooms 320 through 334 (see floor diagram Appendix D). In addition, Room 317 is a locked data center which does not house any staff, only equipment.

It is recommended that offices 323 thru 330 should exit through the side door at the north end of the 1st floor of the Annex. Offices 320 thru 322 and offices 331 thru 333 should exit through the doors on the west side of the 1st floor of the Annex. [see Appendix D]

In the event of an emergency, personnel have been assigned the task of insuring that the offices have been evacuated.

#### ***Responsible emergency evacuation staff:***

West Side Offices

Paul Hudy (alternate Steven Hopper) Rooms 320 through 327 and 334.

East Side Offices

John Leydon (alternate Jo Ann Pearson) Rooms 328 through 333.

## 3.2 HARDWARE FAILURES

UNC-GA maintains a hot-site at MCNC (RTP, NC) in cases of catastrophic failure of the information technology facilities at UNC-GA. UNC-GA technology operations can run indefinitely from these facilities.

### **For short-term or routine failures, computers and peripherals are maintained as follows: Computer Room UPS and Generator**

The UPS in the server room is a **PowerWare 9170+**, serial number **C661N018KH021125**. For maintenance call Eaton (800-356-5737) or National Power Corp 1-800-790-1672. The contract is for Eaton but was purchased through National Power Corp. Maintenance is under PO # W000717 which extends contract to 6/24/2012 (2 yr On-Site Gold plan). The primary technician who shows up is Verne Dregalla (cell 919-618-2313). This information is located and updated at [wiki.northcarolina.edu](http://wiki.northcarolina.edu)

The generator behind the Annex is a **Generac 3848510100** 125KW generator, serial number **20760603**, and our customer number is **104220**. Current contract ends Apr 30, 2015 (PO #W000716). Service contract is a 5 yr Gold Plan (G101-200KW). For maintenance call National Power Corp 1-800-790-1672. Our primary contact is David Fitzsymons, telephone 919-861-6926. **Emergency off-hours** generator service contact number is 1-888-646-8596. This information is located and updated at [wiki.northcarolina.edu](http://wiki.northcarolina.edu)

### **Cisco equipment**

Cisco TAC tele # 1-800-553-2447

We have three Smartnet contracts purchased thru NWN Corp (PO # W100094).

- SmartNet Contract # **91010949** (S2P 24x7x2hr) -- covers the 4506's and the NetFlow cards, 3825 at the tower, ASA5510(bannerVPN), ASA5510(DR site)
- SmartNet Contract # **91010948** (SNT 8x5xNBD) -- covers the 4503, 2921, ASA5510(UNC-GA vpn)
- SmartNet Contract # **91010946** (SU4 24x7x2hr) -- covers the ASA 5520(UNC-GA primary FW); This information is located and updated at [wiki.northcarolina.edu](http://wiki.northcarolina.edu)

### **BlueSocket**

- BSC-1200 serial # 12004907010379 located at the President's house. P.O. # W120513 runs to 1/2/13
- BSC-1200 serial # 12001111010379 located at CSLD. P. O. # P120148 runs to 10/13/14
- BSC-1100 serial # 11011604000010 located at UNCGA, server room 317.
- BSC-1100 serial # 11011604000013 is the backup located in room 022.

For Support call ADTRAN Custom Extended Services 1-888-874-ACES. This information is located and updated at [wiki.northcarolina.edu](http://wiki.northcarolina.edu)

### **Computer Room Air Conditioning**

Computer Room AC is provided by the Liebert Mini-Mate and the Liebert Challenger. The Mini-Mate unit is maintained by UNCCH Physical Plant; Phone number is 800-274-7799;



Computer room is Room 317, Building #499; UNC-GA Customer Number is 0003-001. The Liebert Challenger unit is maintained by Newcomb & Company. Information on both units can be found at [wiki.northcarolina.edu](http://wiki.northcarolina.edu).

### **Systems/Server Infrastructure: Dell Servers and Tape Drive – UNC-GA and MCNC Hot-site**

Each unit is under a maintenance agreement with Dell Computer; Phone number is 800-274-7799. UNC-GA customer number is 017933361. Each unit has its own individual contract based on the individual service tag number for the specific hardware. Service tags and server hardware inventory are located and updated at [wiki.northcarolina.edu](http://wiki.northcarolina.edu).

For routine hardware failures, the hardware can be repaired or replaced quickly enough not to warrant switching operations over the hot-site at MCNC.

## **SECTION 4 - REDUCING RISKS**

### **4.1 PROTECTION OF COMPUTER DATA**

Computer data is protected by a combination of backup procedures and offsite storage of archival backup sets. Data is copied from the hard drives of the computer systems in the General Administration (UNC-GA) Computer Room (room 317, first floor annex, Spangler Center) to removable media so data that is lost or damaged for any reason can be restored. Offsite storage for magnetic tapes (or other forms of information) protects the data in the event that the computer itself is destroyed due to a disaster in the computer room. No organization is likely to recover from a disaster if it's vital records are destroyed. However, recovery is possible when data is protected at another location.

#### **4.1.1 BACKUP PROCEDURES**

Every two weeks a full backup is made of the data on the servers in the UNC-GA Computer Room. This procedure takes place every other Tuesday. Every night an incremental backup is run on the current full set to copy any changes to the data. The backup system is a Dell Powervault ML6000 hardware running Commvault software.

Iron Mountain (<http://www.ironmountain.com>) collects the complete tape backup set every two weeks from the UNC-GA Computer Room and stores it off-site. Tape backup sets are stored separately, so that there are multiple sets of archives increasing with the passage of time. The tapes are recycled in a time period consistent with UNC-GA document retention requirements. The tape backups are synchronized so that the transfer to Iron Mountain occurs on the same day that a new full tape backup set is created locally. The active daily backup sets are stored in the UNC-GA computer room in the Dell Powervault system until it is transferred to Iron Mountain. In addition to tape backup and off-site storage, daily real-time backup for critical data is accomplished through mirroring the data and systems at the UNC-GA Hot-site.

#### **4.1.2 OFFSITE BACKUP RECOVERY PROCEDURES**

Indexing by the Commvault software allows the identification of specific tapes based on the stored data characteristics such as file name, creation date and server volume origin. Retrieval of data stored off site by Iron Mountain is accomplished by authorized request via a web form indentifying tape number and date. Authorized personnel are Paul Hudy, Chris Kerr, and Doug Taber.

### **4.2 PROTECTION OF THE UNC-GA COMPUTER ROOM**

#### **4.2.1 PHYSICAL SECURITY**

Access to the UNC-GA computer room is controlled by an integrated keypad lock. Access by UNC-GA staff is limited to only the individuals that have authorized operational needs. The UNC-GA building itself has controlled access by use of a keycard system, and only currently employed UNC-GA staff have access.

The UNC-GA computer room is also protected by a Netbotz camera system that can be monitored in real time as well as producing periodic images that are sent to authorized personnel for archive and review if needed. Alerts are also generated if there is a noise that exceeds a set threshold, or if the computer room temperature or humidity strays out of a defined range.

The computer room also has a fire detection and Halon fire suppression system. Inspections of this system are performed every six months by BFPE International. If smoke is detected, horns will sound inside and outside the computer room. A zone detection panel located in the computer room indicates which detectors are in alarm condition. The detection system is connected to the building alarm system which will automatically send the alarm to the UNC Chapel Hill Campus Police who are responsible for notifying the local fire department. A handheld fire extinguisher is located in the adjacent room (316). Smoking is prohibited within 100 feet of the building.

The risk of naturally occurring flooding at the Spangler Center is highly unlikely without a prior closing of the facility due to an adverse weather event. If such event should occur, the employees will follow established evacuation routes.

If man-made leaks or flooding is detected, staff will immediately call UNC Chapel Hill Physical Plant. (919) 962-3456 and then UNC-GA IR staff should be notified to assess risk to any information technology resources.

In the case of local and regional electrical outages, the computer room will automatically switch to UPS power and then to generator power. The computer room will return to local “line” power once the system detects that power has been restored and has been stable for a period of time. The generator is powered by a natural gas pipeline, thus the computer room can operate in “generator mode” for an indefinite period of time.

See SECTION 3 - GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS for more details of these systems and procedures.

#### **4.2.2 ACCESS SECURITY**

Access to computer records is controlled by the use of login procedures (IDs), passwords, other access restrictions provided by system software, and manual procedures for the control and restriction of access information.

Access to the computers is controlled by passwords. Each user is assigned a unique user ID and password. Users must change their assigned initial password on their first login. These passwords are subject to password complexity rules adopted by the UNC-GA IR department. Passwords are set to expire after 90 days. Privileged accounts expire every 30 days. Users are encouraged to protect their passwords.

Any accounts issued to staff that are no longer employed by UNC-GA are deleted on the termination date of that employee.

### **4.3 BACKUP OF DATA, HARDWARE, SUPPLIES & DOCUMENTATION**

All information and materials which have been identified as critical for the disaster recovery process are stored offsite.

#### **DATA AND SOFTWARE**

All data resident on the computer(s), including systems software and applications software, are backed up on a routine basis. The Emergency Coordinator is responsible for directing backup procedures. Backup tapes are stored offsite on a periodic schedule as described earlier in this section.

#### **HARDWARE**

Mission critical computer systems are backed up by a contingency computer site (the MCNC UNC-GA Hot-site) as described in section 5. The Emergency Coordinator is responsible for all hardware backup procedures including the availability of the required backup hardware as well as contingency planning for any special peripheral or data communications equipment.

#### **DOCUMENTATION**

Critical operations and applications documentation including The Disaster Recovery Manual resides on the backup tapes in offsite storage. A hard copy of this documentation and the Disaster Recovery Manual is kept at the UNC-GA Hot-site.

## 4.4 INSURANCE

The University of North Carolina General Administration is “self-insured” through the North Carolina Department of Insurance (NCDOI). The on-site insurance officer is Ken Craig. In the event of a loss of equipment, the UNC-GA insurance officer must be notified. The UNC-GA officer will then notify (NCDOI) of a loss. Details of the loss are not necessary at that time.

## **SECTION 5 – UNC-GA “HOT-SITE”/CONTINGENCY SITE DESCRIPTION**

### **5.1 UNC-GA HOT-SITE**

The UNC General Administration (UNC-GA) “hot-site” is located in the Research Triangle Park, NC in building 3 on the MCNC Campus.

The MCNC Data Center resides in the former North Carolina Supercomputing Center two-story building on the MCNC campus at 3021 East Cornwallis Road, RTP, NC. The campus has a single street entrance on Cornwallis Road, and is surrounded by trees in all directions other than the entrance. The Data Center is the site of the former NC Supercomputing Center. Since the transition from the NCSC, the building has been up-fitted with additional electronic monitoring, camera and physical security items, such as barriers at both public and employee entrances. The Data Center itself is entirely on the ground floor with offices for operations staff on the same floor and business related offices on the second floor.

#### **Building Characteristics**

This building is served by Duke Energy, and MCNC has a 1250kva generator and a redundant 900kva battery backed UPS serving both DC and AC to the Data Center Space, and limited AC to the office spaces. HVAC systems include resilient distributions systems in the Data Center itself, with the associated towers in a protected area outside, with a total cooling capacity of 145 tons. In addition MCNC supports cabinet door cooling systems for the highest density blade centers in the Data Center.

The building is watched by MCNC staff both live and on cameras viewed at our Network Operations Centers 24x7, and has card entry security for the building itself and additional card entry security for the Data Center. Card control is strictly followed and enforced among the constituents having a need to enter the Data Center and the MCNC staff. Inside of the Data Center, selected areas are further secured by chain-link fencing, and all constituent's equipment is secured within lockable cabinets.

Each MCNC Data Center constituent is connected into MCNC's NCREN at Gigabit Ethernet or more. There is over 60Gbps of physical external internet and research network connectivity available to carry MCNC traffic from the data center.

The UNC-GA “hot-site” is comprised of 3 racks of equipment within the MCNC data center (see Appendix B). The co-location service for these racks is under an annual, renewable contract with MCNC. The management and administration of servers within these racks is the responsibility of the UNC-GA technical staff. Data replication between the infrastructure located at MCNC and UNC-GA Spangler Center is the responsibility of the UNC-GA technical staff.

In the event of a disaster and as required, office space at MCNC is available to the UNC-GA Emergency Response team for immediate short term technical planning and response purposes. This office space has access to wireless internet service and can be brought on-line in a matter of minutes. The Emergency Response Readiness team (see Section #1) would have sufficient office space for at least 10 team members.

## **SECTION 6 - RECOVERY PROCEDURES FOR A MAJOR DISASTER**

The following contingency plans are for use in a major disaster, that is, a disaster of serious enough magnitude to require activation of the UNC-GA “hot-site”. The procedures described in this section outline the teams involved and the steps to be taken.

### **6.1 EMERGENCY ACTION TEAMS AND RESPONSIBILITIES**

The following Emergency Action Teams have been defined for use in disasters or major emergencies. The purpose, responsibilities, and members of these teams are described on the following pages. The teams will be activated selectively by the Emergency Coordinator according to the nature of the emergency. The teams report to the Emergency Coordinator.

#### **EMERGENCY ACTION TEAMS:**

**Applications Team**  
**Network & Communications Team**  
**Facilities Team**  
**Administrative Team**  
**Systems Team**

The use of Emergency Action Teams and the general responsibilities of Team Leaders are discussed in the following **Sections (6.1.1 - 6.1.5)** Designated leaders are identified in *Appendix E.1 - Readiness Team and Emergency Notification List*

## 6.1.1 APPLICATIONS TEAM

### PURPOSE

The purpose of the Applications Team is to verify proper functioning of the critical applications defined in **Section 2** at the UNC-GA “hot-site” and to coordinate with users about how their applications should be operated during the contingency period.

### RESPONSIBILITIES

- Participate in the identifying of critical systems and the testing of those systems at the UNC-GA “hot-site” as a part of the routine disaster recovery testing.
- In a disaster, whereupon the “hot-site” is activated, verify proper functioning of all critical applications.
- Respond to inquiries concerning any lost work that was in progress at the time of the disaster. When systems are activated at the “hot-site”, the Applications Team must help identify any lost work and assist in the recovery of any work that was in progress.
- Once user work has been recovered, coordinate with the users about any changes in the way they will interface to their applications and provide assistance as necessary.

### TEAM MEMBERS

- Director of Online Services
- Applications Project Leaders
- Programmers & Analysts as required

See *Appendix E.17* for the current team leader.

## 6.1.2 NETWORK & COMMUNICATIONS TEAM

### PURPOSE

The Networking Team is responsible for repair or replacement of network equipment and infrastructure, its installation, configuration, and testing, and all network contingency planning - whether at the original site, or the UNC-GA “hot-site”.

### RESPONSIBILITIES

- Participate in the design and architecture of the UNC-GA “hot-site”. Insure that network equipment and infrastructure are in place to support the recovery of core business operations in the event of a disaster. Participate in disaster recovery testing.
- In the event of a disaster, assess the extent of damage and the affect of failures on computer operations. Assist in making the “go/no go” decision to activate “hot-site” operations.
- Coordinate with vendors in obtaining necessary repairs or replacement of network hardware. Agreements should be negotiated in advance or equipment spared, whenever possible, to rush delivery of equipment in the event of a disaster.
- Coordinate with Purchasing for replacement equipment.
- Install and test all new/replacement network hardware. Provide assistance in other related areas when problems or failures are encountered.

## **TEAM MEMBERS**

- Director, Network & Media Services
- Network Analyst
- System Administrators as required

See *Appendix E.1* for the current team leader.

### **6.1.3 FACILITIES TEAM**

#### **PURPOSE**

The purpose of the Facilities Team is to restore or replace the computer room and other infrastructure facilities that support information technology at UNC-GA, following a disaster.

#### **RESPONSIBILITIES**

- Maintain current configurations of the data processing facilities, either as an appendix to the plan or as part of supporting documentation. These will be stored in the Wiki. The configurations should include space layouts, lists of all facilities, such as air conditioning, power distribution, power conditioning, etc., and specifications of model numbers, capacities, electrical requirements, and so on.



- In the event of a disaster, assess the damage and recoverability of the facilities. If the facility is usable, proceed to organize immediate repairs.
- If the data processing facilities are destroyed and not usable, proceed to locate replacement facilities that can be acquired quickly and used for an extended period if not permanently. Facilities include requisite square footage in a building, cabling, air conditioning, power, etc.
- Coordinate with facilities vendors to provide necessary facilities - build out, equipment, installation, and permits - on an emergency basis. As much as possible, negotiate contingency plans in advance.
- Coordinate with Purchasing for new equipment.

## **TEAM MEMBERS**

- Representatives of UNC Physical Plant
- Director, Networking & Media Services
- Network Systems Manager
- Systems & Network Analyst as required

See *Appendix E.1* for the current team leader.

### **6.1.4 ADMINISTRATIVE TEAM**

#### **PURPOSE**

The Administrative Team is responsible for all activities in the disaster recovery process which are not handled by the other Emergency Action Teams. These activities might include arranging transportation, housing, expense advances, shipping, etc., and performing clerical and other administrative functions.

#### **RESPONSIBILITIES**

- Develop and review administrative procedures of the plan.
- Assist in development of contingency plans as required.
- Handle all administrative arrangements for transportation, housing, shipping, expense advances, etc. Assist in facilitating arrangements, administrative approvals, and so on, with other departments.

- Perform clerical and administrative functions as needed during the disaster recovery.

## **TEAM MEMBERS**

- Associate CIO
- IR Admin Support

See *Appendix E.1* for the current team leader.

### **6.1.5 SYSTEMS TEAM**

#### **PURPOSE**

The Systems Team is responsible for installation, configuration, testing, and replacement of systems hardware and software – whether at the original site or the UNC-GA “hot-site”.

#### **RESPONSIBILITIES**

- Participate in the design and architecture of the “hot-site”. Insure that systems hardware and software are in place to support the recovery of core business operations in the event of a disaster. Participate in the testing and evaluation of the “hot-site” systems hardware and software.
- In the event of a disaster, assess the extent of damage and the affect of failures on computer operations. Play primary role in the “go/no go” decision to activate “hot-site” operations.
- Coordinate with vendors in obtaining necessary repairs or replacement of systems hardware. Agreements should be negotiated in advance or spare equipment should be available, whenever possible, to rush delivery of equipment in the event of a disaster.
- Coordinate with Purchasing for replacement equipment.
- Perform system backups and restores as required.
- Install and test all new/replacement systems hardware. Provide assistance in other related areas when problems or failures are encountered.

#### **TEAM MEMBERS**

- Director, Network & Media Services

- Systems Administrators
- Online Services as required
- Network Analyst(s) as required

See *Appendix E.1* for the current team leader.

## **6.2 NOTIFICATION OF THE READINESS TEAM**

A critical aspect of disaster recovery is quick reaction. This requires immediate notification of appropriate personnel so that the Disaster Recovery Plan can be initiated as quickly as possible.

The Emergency Coordinator has established and will maintain an Emergency Notification List (see *Appendix E D/R Directory*) and will ensure that all key personnel have it available.

### **PROCEDURES**

In the event of a disaster, the following notification procedures will be followed:

1. If the disaster occurs while operations staff is on duty, they should initiate the notification process as soon as possible. If no operations personnel are on duty, a Nagios server at UNC-TV monitors key infrastructure 24x7 and will send alerts to key IR staff who can then begin the notification process.
2. The Emergency Coordinator is at the top of the Notification List. If the Emergency Coordinator cannot be reached, the Alternate Emergency Coordinator or other named persons will be notified until a member of the Readiness Team has been contacted.
3. The first member of the Readiness Team notified is responsible to notify other critical members of the Readiness Team and to initiate action. The initial action will be to confer electronically or via a phone conference the extent of the disaster, followed by the assembling of the team at the UNC-GA “hot-site” or other backup meeting place as determined appropriate.

### **6.3 INITIAL READINESS TEAM PROCEDURES**

Once the Emergency Action Team has been notified, they must proceed to make an immediate assessment of the situation and to initiate appropriate actions.

#### **PROCEDURES**

1. The first member of the Emergency Action Team notified is responsible to notify other critical members of the Emergency Action Team and to initiate action.
2. If the Emergency Coordinator has not yet been reached, the Alternate or persons listed next on the Emergency Notification List will assume full responsibilities of the Emergency Coordinator, until he or she has arrived and been fully briefed. The Emergency Coordinator or acting Coordinator will proceed to implement the disaster recovery plans.
3. Make an assessment of the situation directly at the scene if possible or, if not, indirectly based on reported information from the notification sources.
4. Based on the team's assessment of the situation, determine the severity of the problem and decide on the appropriate action.
5. If the Emergency Action Team member judges the emergency to be a major disaster, proceed to do the following:
  - Notify the appropriate Emergency Action Teams
  - Activate the UNC-GA “hot-site”.
  - Notify top management (*See Appendix E.2*)
  - Notify the offsite storage vendor (Iron Mountain) as necessary.
6. If the emergency is not regarded as a major disaster, then the appropriate correction or contingency plans will be implemented as needed. In such case, selected Emergency Action Teams may still be required and will be notified to take action.

### **6.4 ACTIVATION OF THE EMERGENCY CONTROL CENTER**

In the event of a major disaster, the Emergency Control Center (ECC) will be activated from which all communications and activities can be directed by the Emergency Coordinator (EC).

#### **CONTROL CENTER LOCATION**

The primary Emergency Control Center (ECC) location is building 3 on the MCNC campus at RTP, NC. In the event that an alternate meeting location becomes necessary, the designated EC will select and secure another location.

## **PROCEDURES**

1. The Emergency Coordinator is responsible to maintaining an Emergency Control Center in a state of readiness. The Control Center hosts the UNC-GA “hot-site” systems and equipment, along with a hardcopy of the Disaster Recovery Plan and certain other systems manuals, documentation, software, and supplies that support the contingency effort.
2. The EC must notify the UNC-GA Executive Management that the emergency “hot-site” is being activated. (See appendix E.2).
3. When the Emergency Coordinator has declared a major emergency, the UNC-GA “hot-site” will be activated.
4. All emergency personnel will be notified of the “hot-site” activation and will proceed to the ECC as required.
5. Specific procedures for activating the “hot-site” and continuing operations during the contingency period are outlined in **Section 2.2** of this document.

## **6.5 NOTIFICATION OF EMERGENCY ACTION TEAMS AND TOP MANAGEMENT**

In the event of a major emergency, Emergency Action Teams and top management of the organization will also be notified and apprised of the situation. Top management needs to know about the emergency and the current status of personnel, property, and so on. The Action Teams are intended to carry out very specialized functions in a disaster recovery situation, and will be called in to act according to the emergency.

The Emergency Action Teams are defined in **Section 6.1**. Designated Team Leaders and contact information are identified in *Appendix E.1*.

## **PROCEDURES**

1. Determine which Emergency Action Teams should be activated and if the presence of any top management is required to support the emergency activities or contingency procedures.

2. The Emergency Coordinator should notify top management. The Coordinator or anyone else on the Emergency Action Team can notify other Emergency Action Teams.
3. Top management, names and positions are contained in *Appendix E.2*. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Action Team Leaders. The Emergency Coordinator should inform the top management whether their presence is required and when.
4. In activating the Emergency Action Teams, the Team Leaders of each required team will be called from the Notification List in *Appendix E.1*. Inform them briefly of what has happened, the current status, and the plan of action. Each Team Leader is expected to be prepared to initiate action appropriate to his or her team. He or she is responsible for notifying the team to assemble and act according to their contingency plans contained in **Section 6.8**.

## **6.6 NOTIFICATION OF OFFSITE STORAGE AND CONTINGENCY SITES**

Activation of disaster recovery plans may require retrieval of backup tapes, documentation, and supplies from offsite storage. Personnel at the UNC-GA “hot-site” or other contingency sites will be notified that a disaster has occurred and work space may be required. These tasks will be carried out by specific Action Teams as summarized in **Section 6.8** and detailed in **Section 2.2**.

### **PROCEDURES**

1. Notify the Offsite Storage site(s) that materials will be required to recover from a disaster. (The Offsite Storage site name, address, contacts, and phone numbers are included in *Appendix A.6*.)
2. Notify UNC-GA “hot-site” and other contingency sites as deemed appropriate (see *Appendix A.6*).

## **6.7 SUMMARY OF PROCEDURES FOR CONTINGENCY OPERATIONS**

This section provides an overview of contingency operations once a major disaster has been declared. Detailed instructions on the recovery procedures can be found in **Section 2.2** of this document.

## **SUMMARY OF PROCEDURES**

1. The Networking Team initiates action to make the “hot-site” and its services accessible from the Internet and re-establish VPN tunnels to the campuses.
2. Automated failover will occur for some services (see **Section 2.2.3** for a complete list).
3. The Systems Team will initiate procedures to bring on-line the non-automated failover services (see **Section 2.2.4** for a complete list).
4. All other activated teams will assemble at the designated location Emergency site at MCNC for briefing, discussion of any identified problems, and coordination of the disaster recovery plans.
5. The Applications Team will proceed to identify any work in progress that needs to be recovered and how that can best be accomplished. This will be done based on time of year and the criticality of the application. The Applications Team (via the Internet separately, or having assembled at a Emergency site at MCNC) will verify functionality of the critical systems and applications see **Section 2.1.4**). They will be responsible for notifying the user departments Project Leads to complete the verification process and resume normal operations via systems now running at the UNC-GA “hot-site”.
6. If hardware has been destroyed, damaged, or negatively affected, the Networking Team and Systems Team will proceed to take the appropriate contingency measures to affect repairs to or replace damaged hardware and infrastructure.
7. If facilities have been destroyed, damaged, or negatively affected, the Facilities Team will proceed to take the appropriate contingency measures to repair or replace the affected facilities.
8. The Administrative Team will assist the Action Teams as required.
9. The Emergency Coordinator will keep top management abreast of contingency operations until they can be returned to a normal, non-emergency state.

## **6.8 PROCEDURES FOR REPLACEMENT OF COMPUTER ROOM**

If the computer room is destroyed, steps will be taken to establish a replacement computer room or recover the original site. Computers, air conditioners, power distribution equipment, cabling, etc., must all be considered and installed to prepare for a working computer room.

### **PROCEDURES**

1. The location of a replacement computer room is dependent on space utilization, environmental considerations, and infrastructure requirements. The first alternative will be to repair the existing computer room in **Room 317** of the 1<sup>st</sup> floor annex of the Spangler Center. If this is not possible, a build out of **Rooms 32,33,34** located in the basement of the Spangler Center main building would be the most likely replacement site.
2. If equipment or facilities are salvageable, the Networking, Facilities, and Systems Teams will assess what can be used or repaired and what needs to be replaced. They will initiate all salvage, relocation, and repair activities as necessary.
3. The Networking, Facilities, and Systems Teams will work with the Administrative Team to initiate ordering of all new replacement equipment and facilities on an emergency (rush) basis. Financial and legal issues will be dealt with in this process.
4. As the new computer room is constructed and equipment arrives, the Networking, Facilities, and Systems Teams will coordinate installation, wiring, etc., to ensure that the computer room is configured properly.
5. The Networking, Applications, and Systems Teams will test the readiness of the new computer room. When it is ready, they will initiate procedures to transfer operations from the “hot-site” to the new computer room.
6. The procedures will be complete when all problems with the new computer room have been resolved and operations have been normalized.

## **6.9 PROCEDURES FOR RETURN TO NORMAL OPERATIONS**

The following procedures are for returning to normal operations after emergency (contingency) operations:

### **PROCEDURES**

1. When the computer operation is transferred back either to the original computer room or to a new replacement computer room, employees are to be kept informed. This is the job of the Emergency Coordinator. Data processing staff, users, and management all have an interest and a need to know what is happening. There must be understanding and coordination of changes.
2. As the computer operation is transferred back, the contingency operation will very quickly be phased down. The Systems Team is responsible to use due care and caution to protect all data and software.



3. The Emergency Coordinator and Readiness Team are expected to maintain a full state of readiness during and particularly after returning to normal operations. The Systems Team will begin normal backup and archiving of data.
4. An official statement will be made to all employees stating that the emergency is over and that operations are now or will soon to be returned to normal. The UNC-GA “hot-site” will again assume its secondary role under normal operations.
5. The final activity of the disaster recovery process will be the meeting and debriefing of all Coordinators and Action Teams concerning the activities of the disaster recovery. The Emergency Coordinator is responsible for making sure that events, problems and solutions, etc., are documented. Once documentation has been completed, the Action Teams can be deactivated. During the next review of the plan, the Emergency Coordinator will be responsible to ensure that any lessons learned are incorporated into the plan.

## **SECTION 7 - TESTING AND MAINTENANCE OF THE PLAN**

The Disaster Recovery Plan is not useful until it has undergone an initial acceptance test. The testing verifies that all facets of the plan have been implemented and have been found to be accurate and sufficient. After initial acceptance of the plan, ongoing testing on a periodic basis is required to ensure the continued viability of its contents. The plan must also be reviewed regularly and updated as necessary. This section deals with these issues by providing procedures for testing the plan and for periodic review and update of the plan.

### **7.1 PROCEDURES FOR TESTING**

The Disaster Recovery Plan was tested upon its initial development and will be tested periodically for procedural and organizational aspects as well as the technical ability to process at the chosen contingency computer site.

Because it is important for the emergency teams to remain familiar with the Disaster Recovery Plan and for the plan to reflect the state of computing technology, the Emergency Coordinator is responsible for conducting a test in the year following any substantial change in the computer hardware, applications and systems software, or data communications technology.

#### **PROCEDURES**

1. At least once a year, in conjunction with the process of review and update of the plan, the Emergency Coordinator will design, schedule and notify team members of any testing required. The test may vary from year to year, in order to evaluate different elements of

the plan, but it must address major procedures involving the recovery teams and must test the ability to process at the contingency site.

2. The tests may be organized as several different tests during the year, each testing a different portion of the plan. Regardless of whether or not the plan is tested in phases, at least one of the tests must be performed during a business day to assure that the staff members of UNC-GA are aware of and participate in the effort.
3. The tests are to be regarded as review and training exercises as much as tests of the workability of the plan. However, there will always be some features of the plan, which are truly tested. This means that the tests must be observed, measured, and all successes and failures recorded. The Emergency Coordinator will serve as the test monitor. During the progress of the test, if problems are encountered, solutions will be sought at that time.
4. Each time the computer hardware infrastructure undergoes substantial changes, at least one critical application will be tested at the MCNC contingency site to verify that no technical problems prevent those services from working.
5. Each time a critical application undergoes a new release, it will be tested at the MCNC contingency site to verify that no technical problems prevent those services from working.
6. If results of testing indicate necessary changes to the plan, the Emergency Coordinator will document the recommended changes in the plan and forward to the UNC-GA CIO for approval and addition to the plan. Significant changes will be reviewed in conjunction with UNC-GA Chief of Staff to the President.
7. Changes to the Disaster Recovery plan, which result from the testing process will be incorporated along with the changes from the annual review process.

## **7.2 PROCEDURES FOR REVIEW AND UPDATE**

The effectiveness of the contingency plan is impacted by changes in the environment that the plan was created to protect. Some major factors that will impact the plan are: new equipment, staff and organizational changes, and new or changing critical applications.

The following procedures have been developed to ensure that the plan is reviewed and updated on a regular and reliable basis.

Annually the Disaster Recovery Plan will be reviewed by the Emergency Coordinator and approved by the UNC-GA CIO.

## **PROCEDURES**

The Emergency Coordinator will appoint a review team of one or more people to periodically review and update the Disaster Recovery Plan.

When the review team has completed their review and update process, the Emergency Coordinator will also review and approve the revised Plan.

Once approved by the Emergency Coordinator, the revised plan will be submitted to the UNC-GA CIO for final approval.

The revised plan (after review and update) will be used as the basis of the next scheduled test. Updates to the plan will be distributed to team members prior to the test. However, if the tests themselves also identify changes to the plan, an additional distribution of updates to the plan will occur following the tests.

The Emergency Coordinator will then distribute the revisions to the Plan. For cost considerations, the revisions will be distributed as updates to the previous version.

More frequent reviews/updates of the plan may be initiated by the Emergency Coordinator or Alternate Emergency Coordinator, but any changes will require the approval of UNC-GA CIO.

### **7.3 CRITICAL SYSTEMS TEST PLAN (SEE SECTION 2 FOR CRITICAL SYSTEMS AND APPLICATIONS)**

Annually the Emergency Coordinator will conduct an unscheduled pseudo-test of the D/R “hot-site” preparedness. The test will not actually transfer operations to the MCNC “hot site” but will provide a walkthrough of the steps identified in the Recovery Methodology (Section 2.2 and Appendix C (graphic)).

The pseudo-test will primarily be concerned with the assumed corruption of the live data files and the offsite archival storage tapes will be fetched and restored to the MCNC backup site to ensure validity

Once the backup systems are running at MCNC, accuracy of data between the test system and production will be tested.

Following the test, the Emergency Coordinator will convene a meeting of all participants to discuss what went right and what needs to be modified.

The Emergency Coordinator will be responsible for following up to ensure that all recommendations are incorporated into the Disaster Recovery Plan.

### **7.3.1 CRITICAL SYSTEMS TEST PLAN HISTORY**

The Emergency Coordinator will keep a wiki (wiki.northcarolina.edu) that will log each execution of the critical systems test plan outlined above. This wiki will describe the test performed as well as its outcome. The CIO will review and approve the log every 6 months (July 1 and Jan 1).

## **7.4 RECOVERY TEST PLAN**

A VM Server (VM srv3) was deemed inoperable and critical applications and data considered as corrupted.

The Emergency Coordinator will notify the Systems Team and the Network and Communication Team that a Server failure has occurred.

The Network Team will walk through the procedures for redirecting all internet address (152.4.x.x) to the appropriate substitute address block and do a pseudo-advertisement of the substitute address to the internet.

The automatic failover will commence and the manual intervention processes will be completed to bring the “hot-site” live.

Once the D/R site is live, it will be tested by the appropriate personnel (Administrative Team) for accuracy of data and usability of programs on the system.

The Emergency Coordinator will be notified of the status of the move to the MCNC hot-site and will verify the successful test of each sub-system with the Administrative Team lead.

Upon verifying that all systems were successfully transferred to the D/R site, the Emergency Coordinator will contact the Vice President and CIO with a notification (see example below) of the successful test.

### **7.4.1 LATEST RECOVERY TEST**

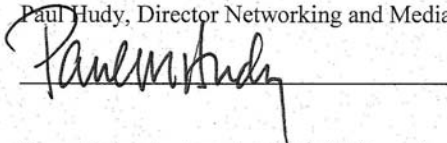
As with the critical systems test plan, the Emergency Coordinator will maintain a wiki that logs each recovery test. The CIO will review and approve the log every 6 months (July 1 and Jan 1).

## 7.5 Signatures

### 7.5 Signatures

The undersigned acknowledge and accept the risks and associated mitigated actions identified in this document.

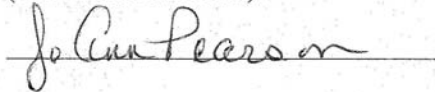
Paul Hudy, Director Networking and Media



Date:

3/7/2012

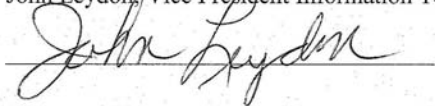
Susan Schwab, Associate Chief Information Officer  
(Jo Ann Pearson Interim)



Date:

3/6/2012

John Leydon, Vice President Information Technology and CIO



Date:

3/5/2012

## 7.6 Revisions

The undersigned acknowledge and accept the risks and associated mitigated actions identified in this document.

John Leydon, Vice President Information Technology and CIO

Revision 1	Initials	<u>JLH</u>	Date:	<u>3/5/2012</u>
Revision 2	Initials	_____	Date:	_____
Revision 3	Initials	_____	Date:	_____
Revision 4	Initials	_____	Date:	_____
Revision 5	Initials	_____	Date:	_____
Revision 6	Initials	_____	Date:	_____
Revision 7	Initials	_____	Date:	_____

Paul Hudy, Director Networking and Media

Revision 1	Initials	<u>PH</u>	Date:	<u>3/7/2012</u>
Revision 2	Initials	_____	Date:	_____
Revision 3	Initials	_____	Date:	_____
Revision 4	Initials	_____	Date:	_____
Revision 5	Initials	_____	Date:	_____
Revision 6	Initials	_____	Date:	_____
Revision 7	Initials	_____	Date:	_____

Susan Schwab, Associate Chief Information Officer  
(JoAnn Pearson)

Revision 1	Initials	<u>JAP</u>	Date:	<u>3/6/2012</u>
Revision 2	Initials	_____	Date:	_____
Revision 3	Initials	_____	Date:	_____
Revision 4	Initials	_____	Date:	_____
Revision 5	Initials	_____	Date:	_____
Revision 6	Initials	_____	Date:	_____
Revision 7	Initials	_____	Date:	_____

## **SECTION 8 - APPENDICES**

### **TABLE OF CONTENTS**

APPENDIX A	COMMUNICATIONS RECOVERY PLAN.....	50
APPENDIX B	UNC-GA DISASTER RECOVERY/FAILOVER.....	51
APPENDIX C	UNC-GA DISASTER RECOVERY.....	52
APPENDIX D	UNC-GA ANNEX 1 <sup>ST</sup> FLOOR.....	53
APPENDIX E	D/R DIRECTORY.....	54
APPENDIX E.1	READINESS TEAM AND LIST OF EMERGENCY NOTIFICATIONS.....	55
APPENDIX E.2	EXECUTIVE MANAGEMENT LIST OF EMERGENCY NOTIFICATIONS.....	56
APPENDIX F	CRITICAL SYSTEMS/CRITICAL APPLICATIONS.....	57

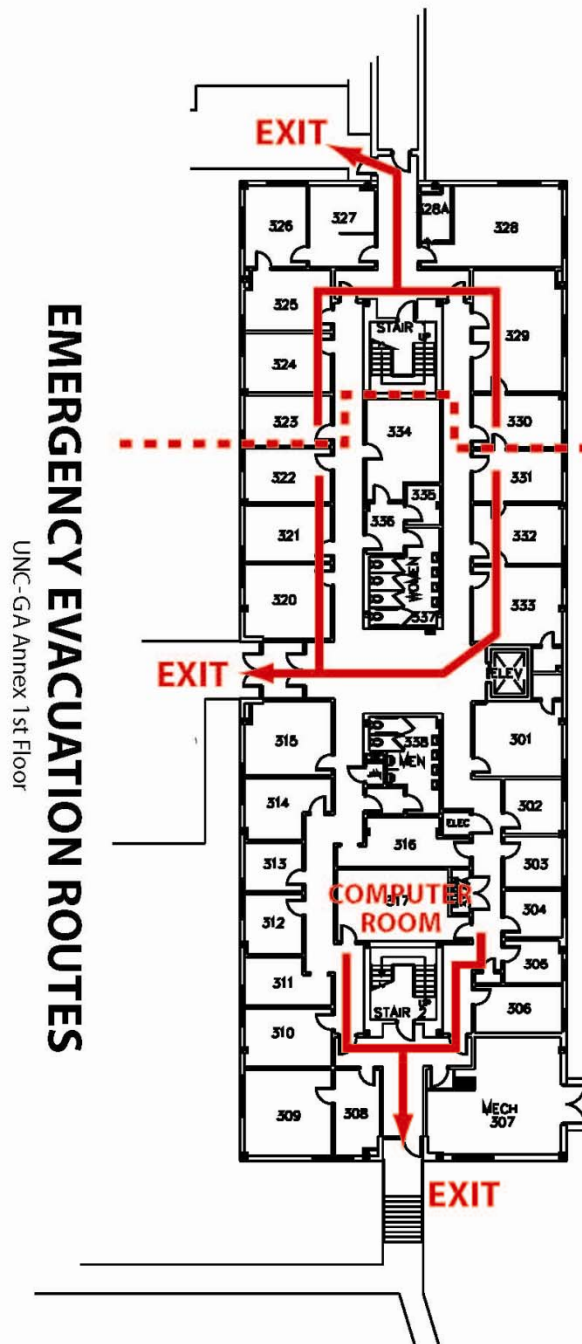
Appendix A Redacted



Appendix B Redacted

Appendix C Redacted

(Appendix D)



**(Appendix E)**

**D/R Directory**

Name	Phone
Shirley Arrington	Redacted
Ginger Burks	Redacted
Alisa Chapman	Redacted
Matt Coffey	Redacted
Lauren Connolly	Redacted
Dan Cohen-Vogel	Redacted
Douglass Davis	Redacted
Karrie Dixon	Redacted
Amanda Dough	Redacted
Dennis Farmer	Redacted
Jeff Hill	Redacted
Steven Hopper	Redacted
Paul Hudy	Redacted
Keith Johnson	Redacted
Kathy Jones	Redacted
Chris Kerr	Redacted
Sofia Kwon	Redacted
Allen Lakomiak	Redacted
Ann Lemmon	Redacted
Alex MacKethan	Redacted
T. Mcmillan	Redacted
Suzanne Ortega	Redacted
Lisane Razack	Redacted
Angelisa Riggsbee	Redacted
Debbie Robertson	Redacted
Robbie Snuggs	Redacted
Chris Stefanick	Redacted
Doug Taber	Redacted
Cody Thompson	Redacted
Christy Tillery	Redacted
Brian Usischon	Redacted
Miriam Tripp	Redacted
Diane Watts	Redacted

**(Appendix E.1)**

**Readiness Team and List of Emergency Notifications.** This list will be reviewed annually to assure that alternates are sufficiently cross-trained to assume responsibilities.

<b>Essential Function:</b>	Emergency Coordinator		
	Primary	Alternate	Second Alternate
<b>People Responsible</b>	Paul Hudy	Doug Taber	Moustapha Barry
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Applications Team		
	Primary	Alternate	Second Alternate
<b>People Responsible</b>	Steven Hopper	Allen Lakomiak	Kenneth Thompson
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Administrative Team		
	Primary	Alternate	Second Alternate
<b>People Responsible</b>	Jo Ann Pearson	Lauren Connolly	Lisane Razack
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Facilities Team		
	Primary	Alternate	Second Alternate
<b>People Responsible</b>	Keith Johnson	Dennis Farmer	Paul Hudy
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Systems Team		
	Primary	Alternate	Second Alternate
<b>People Responsible</b>	Chris Kerr	Doug Taber	Paul Hudy
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Networking and Communication Team		
	<b>Primary</b>	<b>Alternate</b>	<b>Second Alternate</b>
<b>People Responsible</b>	Jim Seals	Doug Taber	Keith Johnson
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Offsite Coordinator (MCNC “Hotsite” Contact)		
	<b>Primary</b>	<b>Alternate</b>	<b>Second Alternate</b>
<b>People Responsible</b>	Todd Broucksou	Network Operations Line	Data Center Help Desk
<b>Phone Numbers</b>	Redacted	Redacted	Redacted

(Appendix E.2)

**Executive Management List of Emergency Notifications.** This list will be reviewed annually to assure that executive management team is current..

<b>Essential Function:</b>	Senior Executives		
	Chief of Staff	SVP Academic Affairs	Vice President and CIO
<b>People Responsible</b>	Jeff Davies	Suzanne Ortega	John Leydon
<b>Phone Numbers</b>	Redacted	Redacted	Redacted
<b>Essential Function:</b>	Executive Assistants		
	Chief of Staff	Academic Affairs	Information Resources
<b>People Responsible</b>	Kathy Jones	Samantha McAuliffe	Lisane Razack
<b>Phone Numbers</b>	Redacted	Redacted	Redacted

## **(Appendix F)**

### **Critical Systems**

#### **A. NETWORK SERVICES**

1. DYNAMIC HOST CONTROL PROTOCOL (DHCP)
2. DOMAIN NAME SERVER (DNS)
3. NETWORK TIME PROTOCOL (NTP)

#### **B. VM WARE**

1. EMAIL
2. MEETINGMAKER
3. ACTIVE COLLAB
4. LIME SURVEY
5. MODEL TEACHER EDUCATION CONSORTIUM
6. GEAR UP
7. SUSPENSION AND EXPULSION
8. FACILITIES MANAGEMENT
9. NC QUEST
10. CAPSTAT
11. EXPANSION BUDGET
12. ENROLLMENT BUDGET
13. HUMANRESOURCES POSITIONS AND PERSONNEL
14. PERFORMANCE EVALUATIONS
15. ORIENTATION
16. STAFF ASSEMBLY
17. OPTIONAL RETIREMENT PLAN (under development)
18. UNC FEDERATION (Shibboleth)
19. WEB SERVICES
20. UNC ONLINE
21. WEBSITE ([www.northcarolina.edu](http://www.northcarolina.edu))

#### **C. UNC ONLINE**

1. PRIMARY WEBSITE([online.northcarolina.edu](http://online.northcarolina.edu))
2. INTERINSTITUTIONAL REGISTRATION SYSTEM
3. EXAM PROCTORING

#### **D. ANCILLARY APPLICATIONS**

1. UNIFIED FINANCIAL DATA MART
2. FILEMAKER PRO

#### **E. INSTITUTIONAL RESEARCH AND ANALYSIS**

1. DIRS Website/ Data Upload and Report repository

#### **F. DATABASE ENVIRONMENT – DEVELOPMENT TOOLS**

1. ORACLE
2. MYSQL

#### **G. SECURITY AND IDENTITY MANAGEMENT**

1. ACTIVE/DIRECTORY
2. UNC FEDERATION (SHIBBOLETH)
3. RADIUS