Like most modern institutions, this college depends heavily on computer-based information systems. Plans must be made to mitigate the effects of disaster and to provide for recovery should a catastrophic event occur. The interruption of computer services for protracted duration is potentially life threatening to any organization; therefore this plan provides the resources to affect an interim solution to maintain mission-critical functions while a computer infra-structure is put back into place.

These are key components in our disaster recovery plan:

- Identify key decision makers
- Define the roles of the Disaster Recovery Team
- Identify key college processes and create contingency plans for each
- Identify sources where emergency processing could be executed
- Provide the means for emergency processing and the eventual rebuild of computing resources

The following pages document these components and form the framework by which decisions are made by the appropriate people. These decisions will be carried out by the Disaster Recovery Team with the contingency plans serving as a guide to restore mission-critical processes. Emergency processing, if needed, will be carried out at the designated host site utilizing the means provided for such an event.
Key Decision Makers
Cape Fear Community College

Dr. Eric McKeithan, President
3200 Shadow Court
Wilmington, NC  28409
350-0862

Ms. Camellia Rice, VP Business Services
305 Rivage Promenade
Wilmington, NC  28412
799-0449

Mr. Carl Brown, VP of Institutional Services
121 Chimney Lane
Wilmington, NC  28409
313-1206

Mr. Dan Hickman, VP of Instruction
123 Colonial Drive
Wilmington, NC  28403
763-1900

Mr. James Parker, Manager of Facilities and Maintenance Services
1811 Wrightsville Ave.
Wilmington, NC  28403
h (910) 762-4360
c (910) 619-0048

Mr. David Chappell, Director of Information Technology Services
401 Columbia Ave.
Carolina Beach, NC  28428
h (910) 458-8786
m (910) 200-4956
N (910)  279-5271
Computing/Telephony Disaster Recovery Team
Cape Fear Community College

David Chappell, Director of Information Technology Services
w (910) 362-7073
h (910) 458-8786
m (910) 200-4956
N (910) 279-5271
   Assess initial situation
   Determines overall level of damage
   Contacts Recovery team

Jakim Friant, UNIX System Administrator (S/A)
w (910) 362-7060
h (910) 686-9819
p (910) 313-3969
N (910) 279-5272
   Assists Director
   Assess specific damage to main Computer System
   Acts as Director in absence of director

Kris Pratt, Network Administrator
w (910) 362-7150
h (910) 395-6091
p (910) 792-3643
N (910) 279-5276
   Assists Director and System Administrator
   Assess specific damage to Network infrastructure
   Acts as Director in absence of director and S/A

Bret Hering, Telephone Tech
w (910) 362-7472
N (910) 279-1899
   Assess specific damage to PBX and other Telephone systems
   Assists Director

Camellia Rice, VP Business Services
w (910) 362-7065
h (910) 799-0449
c (910) 233-9921
   Assists Director in coordination with other divisions
   Assists with Insurance Coverage information
**Larry Butts**, Department of Community Colleges  
(919) 733-7051  
Assists Director and System Administrator in efforts of data and software recovery  
Coordinates emergency processing with Department of Community Colleges as host

---

**Critical Vendors**

**GAServices**  
(888)290-4409  
IIPS Server (sunshine: System id SU713F1152)  
Place ID: 100502  
SUN Maintenance Agreement Number: NK20210849  
Assists with hardware/software recovery

**SUN**  
(800) 872-4786  
Datatel Server (shamash: ESID 31441623, pin #4900)  
SUN Maintenance Agreement Number: NK20143225  
Assists with hardware/software recovery

**Nortel (formerly Periphonics)**  
ESS Enterprise Support System  
(877) 205 5672  
Assists with Telephone Registration recovery

**Mike Cannady**, Consultant, DBM Systems  
w (919) 235-0800  
c (919) 632-7959  
f (919) 235-0801  
Assists with SUN O/S, Application and file recovery

**Sprint**

Assists with PBX systems recovery
Other Important Numbers:

**Borderware** (firewall) Tech support (877) 814-7900 tech support = option 1

**Nokia** (firewall) Customer Service (888) 814-5030 option 2

**Check Point** (firewall) Tech support (817) 606-6600 no more, only sw subscrip

**Cisco** Tech (WAN) p-2014595  cna30685

**Fatpipe** (WAN) Tech support (800) 724-8521 Michael-2261  Dan-2259

**Cable Express** (LAN equipment) (800) 767-3282 ext 2216 Sue Pyle, Danny-2265

**Nortel** (LAN Equipment) Tech support (800) 466-7835 EC 163 SID 81716

**Dell Gold** (Server support) (800) 945-3355

**EIS** (GroupWise support) 452-2692 Matt or Sherry

**Interconnect** (Wiring Infrastructure) (800) 948-0232 x101 Chuck Snider Cell (877) 235-8141

**ENS** (Network Infrastructure) (919) 510-0510 x23 Ike Bunn

**Liebert** (UPS, Envir Cntrl) (614) 738-3651 Jim

---

**Information Technology Services Staff**

*(IT Services)*

**David Chappell**, Director of Information Technology Services  
w (910) 362-7073  
h (910) 458-8786  
m (910) 200-4956  
N (910) 279-5271

**Jakim Friant**, Unix System Administrator (S/A)  
w (910) 362-7060  
h (910) 686-9819  
N (910) 279-5272

**Ashley Do**, Assistant Unix System Administrator  
w (910) 362-7060  
h (910)  
N (910)  

**Kris Pratt**, Network Administrator  
w (910) 362-7150  
h (910) 395-6091  
c (910) 512-3199  
N(910) 279-5276
Donna Grier, Novell System Administrator
w (910) 362-7138
h (910) 793-6699
N (910) 279-5273

Linda Boney, HelpDesk Coordinator
w (910) 362-7188
h (910) 790-9879
N (910) 279-5277

Christina Heikkila, Web Master/Training Coordinator
w (910) 362-7313
h (910) 686-2882
c (910) 231-8804
N (910) 279-1893

Bill Hodder, Hardware Technician
w (910) 362-7061
h (910) 762 2491
c (910) 232-1308
N (910) 279-5265

Matt Rivenbark, Network Technician
w (910) 362-7257
h (910) 602-6788
N (910) 279-5278

Jay Gillock, Software Technician
w (910) 362 7362
c (910) 264-5814
N (910) 279-5275

Matthew Sevier, Microsoft Technical Specialist
w (910) 362-7395
h (910) 397-0448
c (910) 264-6654
N (910) 279-5270

Dom Friant, Computer Tech
w (910) 362-7367
h
N (910) 279-5762
Al Warren, Computer Tech
w (910) 362-7780
h (910) 772-9855
c (910) 471-9855
N (910) 279-5274

Position open, Assistant WebMaster
w (910) 362-7234
h

Joel Brubaker, Information Systems Analyst
w (910) 362-7607
h (910)

Bret Hering, Telephone Technician
w (910) 362-7472
N (910) 279-1899
Contingency Planning for Mission-Critical Processes

Payroll:
If Payroll falls within the disaster period, the Department of Community Colleges will be contacted for further assistance as the host site for emergency processing.

Accounts Payable/Receivable, Purchasing and General Ledger:
Entries will be completed on paper whenever possible. Anything that must be completed on the system would be done after the system is back in service.

Registration:
If registration falls within the disaster period, it will be conducted on paper. Any available personnel will be used to help with this process. When the system is operational, the information will be entered and posted.

Financial Aid and Continuing Education:
Data will be captured on paper as much as possible and input when the system becomes operational.

Mandatory reporting:
The Department of Community Colleges will be contacted immediately to apprise them of the situation and to determine the amount of leeway the school will have on any reports that may become due during this period.

All other Processes:
All nonessential processes will halt until the system is operational. Needed information will be processed, after being deemed essential by the Director, at the emergency processing host site.
In the event of disaster, the system may be recovered or emergency processing performed at the host site by restoring all or part of the data from back-up tapes.

**Tape Backup:**
- A Full Tape Backup of the Administrative Computing System is made daily, Monday-Saturday
- At least one back-up tape per week is stored off-site in a safe-deposit box. Signature card for authorized users contained in appendix.
  
  **Location:**
  BB&T Bank
  115 N. Third St.
  Wilmington, NC 28401
- Daily back-up tapes are kept in a locked storage cabinet or racked Tape Library in the Computer room area

**System Design:**
The Network Infrastructure may be rebuilt from the following documents attached in the appendix to this manual and located in the homes of the Director, System Administrator, and Network Administrator:

- High-level Logical Network Drawing
- IP documentation of various systems
- Model names/numbers of Network equipment

**Data Updating:**
Each Project Manager will coordinate procedures to re-enter lost or updated data. These Managers are listed below:

Camellia Rice: All Financial IIPS/Colleague Modules
Carol Cullum: Curriculum Student Records
Unita Madrey: Continuing Education Records
Procedures

Disaster Preparation:

When a potential disaster is expected, the Unix System Administrator will make two backups and complete an orderly shutdown of the system prior to leaving the college. Power to all servers and network equipment (including UPS’s) will be turned off and un-plugged. The Director will ensure the integrity and security of the Main Communication room and alert Maintenance to install storm shutters, if needed. One Backup set will be taken offsite to the Bank Safe-Deposit Box and the other taken home with the Unix System Administrator. In the event that the Bank is closed, one set shall remain in a secure area within Information Technology Services. If warranted, the Administrative System Servers and staff computers should be protected by covering in plastic obtained form Information Technology Services. All computer-related equipment throughout the college should be un-plugged.

If a disaster is unexpected, such as hardware failure, users should be able to reconstruct any data entered into the system since the last backup once the system has been restored by keeping all source documents readily accessible between backups.

Disaster Recovery:

If the facilities and equipment are usable, the last known good backup shall be restored according to the Contingency Planning and System Recovery processes listed above. The S/A will then verify the integrity of the system. Data lost since the last backup will be recovered via re-entry from source documents. Project Managers (see above) are responsible for their respective data sets and the validation of restored/re-entered data. After the system and data has been validated, the S/A will then inform uses that the system is ready for use.

If the facilities and equipment are not operational, the computer equipment at the Emergency Processing Host Site (above) will be utilized according to the Contingency Plan listed above. Other critical processes identified above will also be carried out according to this plan. All processing completed at the Emergency Host site will be backed up for re-integration onto a newly restored, local system.
Updating:

This document shall be reviewed yearly. After changes are recorded, it shall be re-submitted for approval to the VP for Financial Services under which resides the Information Technology Services. Changes shall be noted by a short description and the date of the change.

Changes to this document:

5-22-05
Added Updating procedure.
Changed name of this document from “Plan” to “Manual”
Updated IT Services Personnel
Updated Computer Services name to Information Technology Services (IT Services)
Appendix additions: Network Closets, Switch Shutdown, E-Mail Templates
Appendix notation of items “on file”
APPENDIX

PBX Procedures
Network Closets
Labs with Switches Shutdown
E-Mail Templates
High Level Logical Network Drawing (on file)
Various IP Listings, including Network Eq. (on file)
Copy Maintenance Agreement for Administrative Computing Systems (on file)
Copy Safe Deposit Box Access (on file)
Nextel Numbers (on file)

Items on file are not included for security reasons. They may be reviewed after clearance with IT Services
Main PBX Shutdown Procedure

PBX may be brought down without regard to Remote Shelves located at BIG & Ncampus, ie; timing does not matter.

Front of unit: faces Terminal and phone on inside wall
Rear of unit: faces outside wall and has power to UPS

1. Down the Network
   route = PBX room > GA Comm Room > Main Campus MDF > NCampus MDF

2. Down the 2 PC’s
   Call Pilot Server (NT Server in corner)
      Stop running Applications
      ShutDown
      Kill power switch
   Management Server (Win2000 running Optivity, near door)
      Stop all running process **except** for Scheduler
      ShutDown
      Kill Power Switch

3. Down the PBX by killing power
   Remove all covers front side (facing terminal and phone) to expose switches
   Kill power in this order:
      Tall Tower, top left – kill 2 breakers
      Short Tower, top right - kill breakers
      Short Tower, bottom right – kill breakers
      Tall Tower, middle and bottom – kill both of these at the same time
   Fans in bottom will continue to run – its OK
   Remove 2 Floppy disks in separate drives located in Tall tower
      Store in safe place
      Disks are the same

4. Remove power from systems (PBX, 2 PC’s and connected peripherals on same UPS)
   Remove plug from UPS to wall receptacle (PBX now on Battery)
      Large plug in center, rear… it is a locking plug…twist to remove
   Kill power from batteries – throw white breaker on back of UPS Battery cabinet.

   PBX and PC’s now Down

5. Turn off Dumb Terminal via front panel switch
   Leave on modem sitting underneath

Procedure now complete
Main PBX Start up Procedure
PBX **must** be up prior to starting Remote Shelves located at BIG and NCampus

1. **Make certain the network is up**
   route = PBX room > GA Comm Room > Main Campus MDF > NCampus MDF

2. **Bring Up the Power**
   Plug the UPS back into wall receptical… it is a locking plug- insert and twist to lock
   Turn on the Batteries by flipping white breaker on back of UPS battery cabinet
   **Do not proceed with next step until fans in PBX hace spun up to speed completely and are circulating air**

3. **Bring up the PBX** (once fans are operational)
   **Insert floppies** (from storage in safe place) back into drives within Tall Tower
   Turn on Power in this order:
   Tall Tower, middle **and** bottom – turn on both of these at the same time
   Short Tower, bottom right – turn on breakers
   Short Tower, top right - turn on breakers
   Tall Tower, top left – kill 2 breakers
   LEDs on cards will be red and will go out as systems boots except for:
   - LED on Tall Tower, bottom - #4 card
   - LEDs on Tall Tower, middle and bottom units - #12
   **PBX takes aprox 30 min to Boot**
   Replace covers front side

4. **Bring up the 2 PC’s**
   Call Pilot Server (NT Server in corner)
   Press power switch
   Login
   username: XXXXX
   password: XXXXX
   All needed Applications should start and become operation within 10 minutes
   Management Server (Win2000 running Optivity, near door)
   Press Power Switch
   Login
   username: XXXX
   password: XXXX
   Scheduler should come up on own
   Start OTM
   Login
   username: XXXX
   password: XXXX

5. **Turn on Dumb Terminal**

   Procedure is now Complete

**Remote PBX Shelf Procedure**
Shutdown
Shutdown is not sequence sensitive

Open both doors
Kill both switches at same time
N Campus (only)- unplug spike strip from wall receptacle

Start Up
Start up **is** sequence sensitive

Determine that the PBX is up and fully operational

Determine that the network is operational
- N Campus Core Switch, Routers and CSU/DSU’s are operational
- N Campus T-1 “Smart Jacks” is operational
- Main Campus “Smart Jacks” operational
- Main Campus Routers, CSU/DSU’s and Core Switch all operational
- GA Rack up and running (pass through route from PBX room to MDF)
- BIG Shelf is not N Campus or GA Rack sensitive

N Campus (only) - re-plug spike strip

Turn both switches inside shelves on **at the same time**

Remote Shelves take approx 10 min to boot
Network Closets – Main Rack Rooms (only)

A-Building (Galehouse) (2)
A214 – MDF

S-Building (McLeod) (3)
Bond Room (S007) – IDF
S200 – IDF
S500 – IDF

N-Building (1)
2\textsuperscript{nd} floor -- IDF

GA-Building (1)
GA Bldg – IDF

L-Building (2)
2\textsuperscript{nd} floor wing – IDF (231)
LRC 2\textsuperscript{nd} floor – IDF

Business & Industry Center (1)
BIG – IDF

E Bldg. – IDF (1)

North Campus (2)
MDF – 2\textsuperscript{nd} floor
IDF – 1\textsuperscript{st} Floor
Labs with Switches to be Shut Down

A Building:

Machine Shop Lab
A316
A402
A411

S Building:

S120 (need key)
S306
S308
S403
S405
S407
S500
S502
S503
S508
S509
S513
S515
E-Mail Templates

BAGS EMAIL:

Bags are available at the Computer Services Help Desk Main, Main Campus and in the Computer Services area at the North Campus (Room NA117) Use these to protect your computer, monitor and/or printer from possible damage should the need arise during the hurricane.

Computer Services is now in the process of delivering bags to the various labs on campus. If you see our personnel making the deliveries, ask them for bags to cover your own computer/monitor/printer. If you miss our folks, come to the HelpDesk of Computer Services, we have some there. It would be best, however, if each department designate an individual to pick up an appropriate number of bags for their area from the HelpDesk.

**Important** make certain the equipment is off prior to bagging!

Guidelines:

- Bag the equipment if the area has a window.
- Bag the equipment if you are on the top floor of a building.
- Bag the equipment if you are in a single-story building

- Those offices whose computers are on the ground floor under a desk may want to raise the computer off of the floor by placing a flat object (such as a phone book) under the computer. In this case, Bag the monitor and keyboard if warranted. On any level, if your computer is on the floor and situated close to a window, you may want to raise it off the floor a bit.

- Disconnect the electrical power from the computer equipment at the wall receptacle **if at all possible**. This will protect the equipment from severe electrical surges and from becoming a shock hazard should the floor become wet. Labs whose computers are in rows will have in most cases have only two electrical connections at the wall end of every row. Your help is greatly appreciated!
E-Mail Templates

Servers Going Down:

All servers - Novell, SUN, Datatel, Web, BlackBoard, etc will be going down today at 5:00PM.

The network which supports these servers and our computers that connect to them is also going down at 5:00PM.

The PBX system which runs the phones on the Main and North Campuses will be going down at 5:00PM.

Instructors with first classes in the Computer Labs are asked to remove the plastic bags form the computers and plug in the equipment wherever possible. If you need help or have questions, please call the HelpDesk at 7188.

It is our goal to have these systems running as early Friday as possible. Should circumstances fall where everything is not completely operational by 8:00AM, we will do out best through whatever means available to alert you to the status of these systems.

Good Luck to us all!