Mitchell
COMMUNITY COLLEGE

Risk Assessment and Business Continuity Plan
2011-2012
January 4, 2012

Background and Terminology

The North Carolina Community College System (NCCCS) mandated in 2004 that each college should implement an appropriate Financial Services Continuity Plan to "ensure the timely delivery of critical functions and services to its stakeholders". The Business Continuity plan must identify and classify risks as well as appropriate risk mitigation. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the operational continuity of critical college systems and resources.

At a minimum, the NCCCS recommends the college's Business Continuity Plan should:

Define the college's critical functions and services.

- Define the resources (technology, staff, and facilities) that support each critical function or service.
- Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority. (For example – registration, payroll, reporting deadlines, etc.)
- Provide a disaster recovery plan for all critical functions and services including the required facilities and resources.

The Office of Institutional Technology (ITS) defines **risk** as the exposure of an activity to potential damage. Three broad categories of risk have been identified for purposes of this plan.

- **Financial Services Risk**—The cost and/or lost revenue associated with an interruption to normal Financial Services operations.
- **Organizational Risk**—The direct or indirect loss resulting from one or more of the following:
  - Inadequate or failed internal processes
  - People
  - Systems
  - External events
- **Information Technology Risk**—The loss of an automated system, network or other critical information technology resource that would adversely affect Financial Services processes.

Critical functions: The administration and appropriate employees were asked to identify the processes and activities within their work units that were necessary for the delivery of instruction and the supporting operations of the College.

Risk assessment: In assessing risk, two primary questions are considered. First, how serious is the damage that could be caused by the situation or activity? Secondly, how likely or unlikely is it that the situation or activity causing the potential damage will occur? Positive answers to both of these questions indicate a situation which requires a contingency plan to insure the continuation of the College's critical functions. This analysis also helps to determine where improved internal controls or redundant systems are required that may prevent potential dangerous situations. The administration and appropriate staff were asked to identify the likelihood and severity of impact to critical functions under three broad scenarios:

1. The loss of access to currently needed facilities for an extended time (in excess of a week).
2. The loss or extended absence of a key employee.
3. The extended failure of critical systems, including electricity and computer networks.

Disaster recovery refers to a coordinated institutional response needed to assess the damage of an event, reduce the time without services or operations, and to implement the continuation of effective services and operations. Using the risk assessment information, contingency plans and disaster recovery plans have been developed to address those risks with a significant likelihood of occurrence and an operational impact.

Curriculum Instruction Area

Instruction

Critical Function: To provide instruction for all curriculum programs.
Maximum amount time area could operate without function: None
Major Threats/Plan:

Facilities: **Threat:** Limited access to instructional areas. For example if a building was not accessible as a result of a disaster such as the Grier Science Building, where the nursing classrooms and labs are located. **Plan:** Classroom instruction would be moved to another building and a mock lab could be set-up if equipment was still accessible. If equipment was not accessible arrangements would be made to rent equipment or use equipment from a local healthcare agency, such as Iredell Memorial Hospital.
Personnel: **Threat:** Resignation or long-term absence of a faculty member. **Plan:** The office of the Vice President for Instruction will maintain a database of the names, contact information, and credentials for adjunct faculty.
Technology: **Threat:** The server for Black Board courses is not functioning. **Plan:** Have available a back-up server or alternate way of delivering instruction via distance learning.

Critical Function: Maintain current approved Programs of Study (POS) for all curriculum programs.
Maximum amount time area could operate without function: One semester or until required curriculum change needs to be approved prior to implementation.
Major Threats/Plan:

Facilities: **Threat:** Limited access to curriculum area that maintains POS. **Plan:** Contact the Academic and Student Services Division of the North Carolina Community College System Office for a copy of current POS.
Personnel: Threat: Key personnel resign or long-term absence. **Plan:** Cross-training.
Technology: Threat: Malfunction of POS or Common Course Library software. **Plan:** Submit paper versions of POS changes to the System Office for review and approval prior to implementation.

Critical Function: Faculty Contracts
Maximum amount time area could operate without function: None
Major Threats/Plan:

Facilities: **Threat:** Limited access to curriculum area that generates faculty contracts. **Plan:** Access system from another computer terminal.
Personnel: Threat: Key personnel resign or long-term absence. **Plan:** Cross-training.
Technology: Threat: Malfunction of software. **Plan:** Create paper versions of contracts based on the schedule.

Curriculum Instruction Area
LRC

Library

Critical Function: To assist students with their research needs.
Maximum amount time area could operate without function: None
Major Threats/Plan:

Facilities: **Threat:** Loss of access to library.
Plan: Students could access NCLIVE and the on-line catalog from any computer located elsewhere on campus. If long term, arrangements would be made with area libraries to provide off-site service

Personnel: **Threat:** Resignation or long-term absence of a librarian.
Plan: The Director of the LRC will coordinate, using backup system of LRC staff. All LRC staff is trained to provide services to students. In addition, English professors would assist with high-level research needs.

Technology: **Threat:** Internet access is interrupted campus wide.
Plan: Library Internet service would be recognized as a high priority in a technology recovery plan. Students would be directed to their area libraries for temporary Internet access.

Critical Function: Building and maintaining the library's collection
Maximum amount time area could operate without function: Two days.
Major Threats/Plan:

Facilities: **Threat:** Loss of access to library.
Plan: Temporary loss of access would require students to temporarily use other area libraries, coordinated by the Director of the LRC. Permanent loss of the facility and its contents would require replacement of the library's collection.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Director of the LRC will coordinate, using backup system of cross-trained LRC staff.

Technology: Threat: Loss of on-line catalog.
Plan: Provide extensive student support from library staff.

Curriculum Instruction Area
LRC

Critical Function: Maintaining circulation records of users
Maximum amount time area could operate without function: Two days
Major Threats/Plan:

Facilities: **Threat:** Loss of access to the LRC.
Plan: Use off-site access to SIRSI computer system

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Director of the LRC will coordinate, using backup system of cross-trained LRC staff.

Technology: Threat: Loss of access to SIRSI and Datatel
Plan: Maintain an index file on each end user when the system is down.

<u>Developmental Studies</u>

Critical Function: Providing tutoring services to curriculum students.
Maximum amount time area could operate without function: None when classes are underway.

Major Threats/Plan:

Facilities: **Threat:** Loss of access to the LRC.
Plan: The Director of the LRC and the MIND Center will work with the administration to identify and implement temporary locations and hours of operation on campus in the event the LRC building is inaccessible.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Director of the LRC will coordinate, using backup system of cross-trained LRC staff, supported by the Vice President for Instruction and faculty as needed. Use of volunteer tutors to supplement paid staff.

Technology: Threat: Loss of access to lab computers and network
Plan: Identify location on campus with computers to provide temporary services.

Continuing Education

Critical Function: Provide instruction and training to students in the continuing education programs.
Maximum amount time area could operate without function: None.

Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Vice President of Continuing Education and the directors of the respective programs will work with the administration to identify and implement temporary locations and hours of operation on campus in the event regularly scheduled buildings are inaccessible, including a use agreement with the Iredell/Statesville and Mooresville Graded Schools school systems for use of available school facilities and vacant commercial properties.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Vice President of Continuing Education and the program directors will coordinate; using temporary instructors and revised work schedules to cover for classes taught by absent personnel or vacated positions. Employees performing administrative or support functions will be cross-trained in order to temporarily backup critical non-instructional functions, such as registration and payroll.

Technology: Threat: Loss of access to lab computers and administrative network.
Plan: Identify and implement location on campus with computers to provide temporary services. The Vice President of Continuing Education and the program directors will coordinate implementation of recovery plan with Director of Information Systems.

Student Services

Veteran

Critical Function:

To provide on-line certification for veteran students through VA-ONCE

Maximum amount of time area could operate without function:

30 Days

Major Threats/Plans:

1) **Facilities Threat:**

Limited access to veterans' records. For example, if the Main Building was not accessible as a result of a disaster.

Plan:

Veterans' records could be accessed through any computer with Internet access. If campus equipment was not accessible, arrangements could be made to rent equipment. We will immediately investigate purchase of fireproof file cabinets. To some extent our ability to re-create records is contingent upon our being able to access the registrar's academic records for veteran students.

2) **Personnel Threat:**

Resignation, death, or long-term absence of VA certifying official

Plan:

The VA certifying official will maintain a database of contact information on certifying officials at other colleges who could be brought in as substitutes and/or for the training of additional personnel.

3) **Technology Threat:**

The server is not functioning or not accessible.

Plan:

Have available a back-up server or alternative equipment for accessing VA-ONCE.

Student Services

Financial Aid

Critical Function:

To provide financial aid services to students during the fall, spring, and summer registration periods in coordination with the Financial Services and Registrar's Offices.

Maximum amount of time area could operate without function:

Registration could be delayed for only a short period of time (an hour or less). It would be imperative to go forward with a manual registration process in a major technological breakdown.

Major Threats/Plans:

1. **Facilities Threat:**

   No access or limited access to the Main Building as a result of a disaster or hazardous condition.

   Plan:

   If the College's computer system can be accessed in another building on campus, the financial aid operations would move in coordination with the Financial Services and Registrar's Offices. Additional College personnel would be used to direct the flow of student traffic.

2. **Personnel Threat:**

   Resignation, extended illness, or death of key personnel in the Financial Aid Office during registration.

   Plan

   Cross training has already begun within the Financial Aid Office. The Assistant Director of Financial Aid is able to maintain the operations of the office in the absence of the Director. The Financial Aid Assistant is also trained in all operations of the office.

3. **Technology Threat:**

   Computer access is not available due to problems with the campus server.

   Plan:

   The College's "Emergency Registration Plan" would be put into immediate action with the Dean of Student Services and the Director of Financial Services coordinating with the Director of Financial Aid.

Student Services

Registration

Critical Function:

To carry out the registration process in the fall, spring and summer semester with coordination of the instruction, faculty, Financial Services office, counseling and financial aid areas.

Maximum amount of time area could operate without function:

To assure the continued educational standards of this process only an hour or so would hinder the whole process. It would be imperative to go forward with a manual function in a major technological breakdown. Forces other than technological would have to be determined by the facilities plan.

Major Threats/Plans:

1. **Facilities Threat:**
   Limited access to the Main Building should something happen to the structure, foundation or the accessibility of the building.

   Plan:
   If computer access is still available on campus, we would move to another building, set up using available technological resources, post personnel to help with the flow of student traffic and still register on the computer if possible.

1. **Personnel Threat:**
   Sudden illness, death or extended illness of key personnel in Registrar's area during registration, end of semester or graduation.

   Plan:
   Cross training in the new system has already begun and will continue to do so as we move toward that system. The new system also provides Continuing Education personnel key functions regarding records and registration—those personnel could be utilized in an extreme emergency and vice versa if a problem arose in the Continuing Education unit during an extended period of time. Other Admissions/Registrar personnel are also able to step in and keep the area functioning in case of absence of the Registrar.

2. **Technology Threat:**
   Computer access is not available due to problems with the on campus server.

   Plan:

In the case of registration, an Emergency Registration Plan would be put into immediate action with the Dean of Student Services and the Vice President for Finance and Administration coordinating with the Director of Admissions to start a manual process. All staff employees of the college would be expected to work both day and evening processes to handle the manual flow.

A. Faculty: will proceed as usual with the advising of the students in normal stations. Students would pick up their advising materials from the usual station and would proceed to orientation and then to advising with their faculty advisor.

B. Student Development: If the computer fails during Early Scheduling and Advising, students will complete the process as usual and the schedules will be input in the system as soon as the problem is resolved. If the computer fails on Registration Day or during the Drop/Add process where it is vital that courses be input for the start of instruction, the following steps shall be followed:

1. At the end Early Advising and Scheduling, the Registrar will run a list of all courses showing the seating availability and if possible an individual unofficial class roster of each course for the term.

2. The class rosters will be used, if available, or individual class rosters will be made for each class and section.

3. Tables will be set up in the most appropriate area of the college with the class rosters. Rosters will be divided in alphabetical order with at least two people manning each table.

4. Students will take the schedule cards completed by the advisor, already ensuring that the schedule is free of conflicts and that pre-requisites/co-requisites have been met, and will go past each table to get their names on a roster. One person will call out the information and the other will write down the name and ID number of the student. The class will be initialed by the person who has written information on the roster. The student will proceed through all tables and the last table will total the credit hours.

5. The student will then be sent to a coping location where the schedule will be copied, a copy given to the students and the original held for the Registrar's Office.

NOTE: In the event the computer goes down during the time that students have already completed early scheduling and official schedules are available, the process will continue for those students as usual with the manual system only used for changes or new students.

Student Services

Counseling Services

Critical Function: To provide placement testing to all incoming students.

Maximum amount time area could operate without function: Depends on Academic Calendar… needed 30 days prior to the beginning of each semester.

Major Threats/Plan:

Facilities: Threat: Lack of access to placement testing center.

Plan: Incoming students could access the on-line placement testing program from any computer located on campus. If long term, arrangements could be made with local public schools or libraries to provide off-site placement testing.

Personnel Threat: Resignation or long-term absence of director of counseling/testing.

Plan: ALL members of the College's counseling staff are trained in administering and interpreting placement tests.

Technology Threat: Internet access is interrupted campus wide.

Plan: Students would be administered a paper and pencil version of the placement test.

Critical Function: To provide legally mandated accommodations to students with disabilities.

Maximum amount of time area could operate without function: None. This office exists to perform this function.

Major Threats/Plan:

Facilities: Threat: Loss of access to disabilities coordinator's office.

Plan: Disabilities coordinator's office would be moved to another campus building.

Personnel Threat: Resignation or long-term absence of disabilities coordinator.

Plan: Cross-train designated counselor to provide disabilities services.

Technology Threat: Inability to access inter-intranet.

Plan: As long as there is a designated disabilities coordinator, the function could be temporarily met by communicating via telephone, written notes and face-to-face meetings.

Critical Function: To provide counseling services to faculty, staff and students in the event of a disaster.

Maximum amount of time area could operate without this function: 1-3 days depending on the severity of the disaster and the number of individuals effected.

Major Threats/Plans:

Facilities Threat: Loss of access to counseling center/Main Building

Plan: Any on-campus location, if available, or any public/church building with a meeting space.

Personnel Threat: All of the College's counseling staff are injured or unavailable for crisis counseling.

Plan: Referrals are made to the Iredell Crisis Information and Referral Service.

Technology Threat: Inter-intranet service is interrupted.

Plan: Through voice mail, personal contact and area newspapers, the availability/location of crisis counseling will be noted.

Administration

Financial Services Office

Payroll and Fringe Benefits

Critical Function: Accurately meet deadlines for employee payroll and fringe benefits.
Maximum amount time area could operate without function: 3-5 days, dependent upon the date of the month.

Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Director of Financial Services, Director of Human Resources and Accounting Specialist will utilize system backups located off campus and coordinate off-site payroll processing with Director of Information Systems and the Systems Office.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Director of Financial Services coordinates the cross training of the Accounting Specialist and the Director of Personnel to insure both benefits and payroll processing can occur in the absence of any person.

Technology: Threat: Loss of access to lab computers and administrative network.
Plan: The Director of Financial Services, Director of Human Resources and Accounting Specialist will utilize system backups located off campus and coordinate off-site payroll processing with Director of Information Systems and the Systems Office.

Cash Receipting

Critical Function: Accurately record and deposit cash receipts.
Maximum amount time area could operate without function: 1 day, in order to remain in compliance with the Daily Deposit Act.
Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Director of Financial Services and Accounting Specialist will utilize networked computers located in another building to process cash receipting .

Personnel: Threat: Key personnel resign or long-term absence.
Plan: Under the supervision of the Director of Financial Services, the AP Accounting Specialist serves as the immediate backup for the AR/CR Accounting Specialist. In addition, the Payroll Accounting Specialist and the Administrative Assistant are trained to receipt funds and to process the bank deposit.

Technology: Threat: Loss of access to administrative network.

Plan: Receive monies using duplicated handwritten receipts and receipt logs. Manual reconciliations conducted by the Accounting Supervisor on a daily basis.

Administration

Financial Services Office

Accounts Receivables

Critical Function: Accurately record and manage student accounts receivables.
Maximum amount time area could operate without function: 1-2 days, dependent upon the date of the month.

Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Director of Financial Services, Director of Human Resources and Accounting Supervisor will utilize system backups located off campus and coordinate off-site receivables processing with Director of Information Systems and the Systems Office.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Director of Financial Services is fully trained to backup the Accounting Supervisor for AR management.

Technology: Threat: Loss of access to the administrative network.
Plan: The Director of Financial Services and Accounting Supervisor will utilize system backups located off campus, and if necessary coordinate account updates through the System Office.

Purchasing and Receiving

Critical Function: Purchasing and receiving of purchased items/services.
Maximum amount time area could operate without function: 3-5 days, dependent upon the date of the month.

Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Director of Financial Services and Purchasing Agent will coordinate with the Director of Information Systems to identify the location and set up the computer equipment needed to process purchase orders and receive purchased items.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Payroll Officer and the Director of Financial Services are able to process purchase orders and receive items.

Technology: Threat: Loss of access to the administrative network.
Plan: The Purchasing Agent will process and receive purchase orders through the E-procurement system off campus through connectivity with the System Office.

Administration

Financial Services Office

Accounts Payable

Critical Function: Accurately process and record accounts payable transactions.
Maximum amount time area could operate without function: 3-5days, dependent upon the date of the month.

Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Director of Financial Services and Accounting Supervisor will utilize system backups located off campus and coordinate off-site vouchering with Director of Information Systems and the Systems Office. Manual checks may be processed as needed.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Director of Financial Services and Accounting Supervisor are fully trained to backup the AP Accounting Clerk.

Technology: Threat: Loss of access to the administrative network.
Plan: The Director of Financial Services and Accounting Supervisor will utilize system backups located off campus, and coordinate with the bank and System Office in processing payments.

Financial Reporting

Critical Function: Accurately process and record accounts payable transactions.
Maximum amount time area could operate without function: 3-5days, dependent upon the date of the month.
Major Threats/Plan:

Facilities: **Threat:** Loss of access to the facilities.
Plan: The Director of Financial Services will utilize system backups located off campus and coordinate reporting with Director of Information Systems and the Systems Office.

Personnel: Threat: Key personnel resign or long-term absence.
Plan: The Financial Analyst and Accounting Supervisor are backups to the Director of Financial Services and are able to perform the monthly reporting duties of the Director of Financial Services.

Technology: Threat: Loss of access to the administrative network.
Plan: The Director of Financial Services will utilize system backups located off campus, and coordinate with the System Office in processing reports.

INTRODUCTION

Purpose

This document includes both an IT contingency plan and a disaster recovery plan for Mitchell Community College. The information present in this plan guides College management and technical staff in the recovery of computing and network facilities operated by IT and in restoring operations resulting from any emergency disruption. This plan also provides for information/procedures that can assist in the prevention or interruption of computer operations as well as for recovery from emergency disruption of computer services. The primary focus of this document is to provide a plan to respond in an orderly way to an emergency that severely impacts the central administrative computer systems and/or campus network operated by the Institutional Technology Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Notification/Activation phase*** to detect and assess damage and to activate the plan
  - ***Recovery phase*** to restore temporary IT operations and recover damage done to the original system
  - ***Reconstitution phase*** to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated personnel and provide guidance for recovering and continuing operations during prolonged periods of interruption to normal operations.
- Ensure coordination with other *MCC* staff who will participate in the contingency planning strategies.

- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Scope

Although this plan includes information and activities dealing with computer resources campus-wide, it is primarily focused toward insuring continued operation of the administrative computing function of the College, critical resources such as the telephone and e-mail systems, and distance learning. The plan will discuss in general terms the policies and procedures that implement risk assessment, information security, disaster prevention and recovery. Specific policies and procedures will be referenced and included in the Appendix.

The primary component of the administrative computing function is the central administrative computer system. This includes the hardware and software systems and the data stored and processed by the system. The primary component of the telephone system is the Cisco publisher call manager and its backup the Cisco subscriber call manager. The primary component of the distance learning system is Moodle. The main thrust of the plan is to protect the data and the equipment that comprise the central computer system, critical system resources, and their operational infrastructure. Planning is also included for communication failure to the primary campus locations. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Definitions

a. Interruption - Any occurrence that prevents a user from completing normal computer operations
b. Emergency - An interruption that potentially can cause serious consequence to the College
c. Disaster - An interruption that prevents multiple users from completing normal computer operations for an extended period of time.

Assumptions

The following assumptions were used when developing the IT Contingency Plan

- Catastrophic long-term disasters in which the College ceases to function for an extended period cannot be planned for. Computer services recovery from such an event will be part of a general recovery process.

- Some risks are acceptable. The College does not possess the necessary resources (financial and personnel) to protect itself against every conceivable risk.

- The campus network or critical server is inoperable at the MCC campus and cannot be immediately recovered.

- Critical Systems/Applications are affected.

- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Contingency Plan.

- Preventive controls (e.g., generators, environmental controls, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.

- Computer center equipment, including components supporting the main campus network or critical server are connected to an emergency generator capable of providing uninterrupted power. Other areas are connected to uninterruptible power supply (UPS) that provide *30 minutes to 1 hour* of electricity during a power failure.

- The campus network or critical server hardware and software at the MCC campus is unavailable.

- Current backups of the application software and data are intact and available at the offsite storage facility.

- Service agreements are maintained with hardware, software, and communications providers that service the College to support the emergency system recovery.

- Natural gas supply to the emergency generator is not compromised.

Evaluation

The Director of Institutional Technology will conduct an annual review of this plan to ensure that the plan is current and that policies, procedures and practices are in place to maintain implementation of the plan.

System Information

Specific system information is considered to be classified information and is not included in this document.

Mitchell Community College

BUSINESS IMPACT ANALYSIS

Description of process and narrative of critical systems:

See "Concept of Operations" for description of MCC Campus systems. Based upon current administrative/instructional operations and workflows and the anticipated impact of loss of IT resources on these workflows a contingency plan has been developed for all identified critical systems.

Campus network stakeholders have been identified as follows:

Administrative Staff, full and part-time
Faculty, full and part-time
Students

Based upon this concept of operations and identified Computer and Telecommunications resources in use by the College, the following have been identified as critical IT resources:

Identify Critical IT Resources (Risk Assessment) 10/27/2011

1. Datatel box
   a. Risk
      i. Loss would mean no payroll, schedules, registration etc (Disaster) downtime of more than 2 days will have severe impact on college operations.
   b. Mitigation
      i. We have a DR box using rsync plus backups and NCCCSO support but the DR box needs to be moved to MB however, with new UI we will need a Datcore DR box as well.
2. Datatel DR box
   a. Risk
      i. This is the box we depend on in the event of a failure of the production Datatel box which makes it pretty important
   b. Mitig ation
      i. If we lose both boxes we will have to use manual processing.
3. Destiny

a. Risk
   i. Loss of DNS and authentication. We have multiple domain servers so the impact of long periods of downtime (more than 2 days) is manageable

b. Mitigation
   i. Alternate DNS and authentication available

4. Hershey
   a. Risk
      i. Total loss stops procurement, stops transcripts, limits HR, Fin Serv, Stu Serv (Disaster) Hershey is not as critical as datatel but downtime of more than a few days will significantly impact college operations.
   b. Mitigation
      i. Backups, VSphere, Hershey support NOT full mitigation
5. Serenity
   a. Risk
      i. Loss of DNS and authentication for students. We have multiple domain servers so the impact of long periods of downtime (more than 2 days) is manageable
   b. Mitigation
      i. Alternate DNS and authentication available
6. Datcore
   a. Risk
      i. Web UI stops working, (once we no longer have old UI Disaster)   downtime of more than 2 days will have severe impact on college operations.
   b. Mitigation
      i. None other than backups
7. WA
   a. Risk
      i. If it fails during registration will stop the process downtime of more than 2 days will have severe impact on college operations.
   b. Mitigation
      i. Backups, VM, long registration windows
8. Blade Enclosure
   a. Risk
      i. Total loss would mean most network services on Main Campus would be gone (Disaster)
   b. Mitigation
      i. We do have alternate source for DNS, DHCP, and authentication but it would be slow
9. EComm
   a. Risk

i. Loss of ability for college to take credit cards, during registration this would be (Disaster) not as critical as datatel but downtime of more than a few days will significantly impact college operations.

b. Mitigation

i. VM, backups

10. Informer
    a. Risk
       i. Loss of ability for users to do reporting and queries once the old UI is gone loss would be (Disaster) not as critical as datatel but downtime of more than a few days will significantly impact college operations.
    b. Mitigation
       i. VM, backups, still have access to old UI for now
11. Exchange
    a. Risk
       i. Loss means no email (Disaster) downtime of more than a couple of days will significantly impact college operations.
    b. Mitigation
       i. We can move everyone to Gmail as long as internet access is working.
12. GW
    a. Risk same as Exchange for now, when the move to Exchange is complete the only real loss would be historical which in the event of litigation could be significant
13. Phone System
    a. Risk
       i. Total loss means no local phone service or VM at the college (Disaster) downtime of more than a couple of days will significantly impact college operations
    b. Mitigation
       i. Redundant CM, GW, and we have lots of cell phones plus SmartNet 8x5 NBD
14. Informacast
    a. Risk
       i. Loss of emergency notification system
    b. Mitigation
       i. VM, backups
15. Moodle
    a. Risk
       i. Loss means DL classes cannot meet (Disaster) downtime of more than a couple of days would significantly impact students abilities to complete coursework.
    b. Mitigation
       i. Cloud based solution with near bullet proof survivability, as far as we know
16. Metro E internet

    a. Risk
        i. Loss means internet access stops severely limiting instructional delivery (Near disaster) not as critical as datatel but downtime of more than a few days will significantly impact college operations.
    b. Mitigation
        i. None other than SLA with MCNC

17. Metro E intracampus
    a. Risk
        i. Loss means no network access for remote campuses not as critical as datatel but downtime of more than a few days will significantly impact college operations.
    b. Mitigation
        i. None other than SLA with MCNC
18. WIFI
    a. Risk
        i. Loss means no WIFI access, at this time the impact of loss is minimal
    b. Mitigation
        i. Multiple controllers and AP's
19. Network core
    a. Risk
        i. Total loss would mean network would stop functioning (Disaster) A total failure has a greater effect than anything else.
    b. Mitigation
        i. We have redundant cores but they are in the same location SmartNet 8x5 NBD
20. Network edge switches
    a. Risk
        i. Could mean loss of a remote campus or lab depending on the switch
    b. Mitigation
        i. Cisco SmartNet 8x5 NBD, spare switches, and could move switches around if needed
21. Border FW
    a. Risk
        i. Loss means internet access stops severely limiting instructional delivery (Near disaster) not as critical as datatel but downtime of more than a few days will significantly impact college operations.
    b. Mitigation
        i. Cisco SmartNet 8x5 NBD
22. Unix FW
    a. Risk

i. Loss would mean Datatel access is lost. Not as critical as datatel (we could change datatel config to run without FW) but downtime of more than a few days will significantly impact college operations.

b. Mitigation

   i. Cisco SmartNet 8x5 NBD, could reconfigure to run without FW, could steal one from somewhere else

23. Donor2
    a. Risk
        i. Loss means no access to Donor database or accounting system
    b. Mitigation
        i. Support agreements with Donor2 and Great Plains, backups
24. Donor2 FW
    a. Risk
        i. Would prevent access to Donor2 and Great Plains in the event of total loss
    b. Mitigation
        i. Cisco SmartNet 8x5 NBD, spare FW, could remove FW and run open access
25. Booklog
    a. Risk
        i. Total loss would shut down Bookstore, if this happens during the first week of the semester it would be a (Disaster) not as critical as datatel but downtime of more than a few days will significantly impact college operations.
    b. Mitigation
        i. Backups, support with Booklog, could move to another server
26. Booklog FW
        i. Total loss would shut down Bookstore, if this happens during the first week of the semester it would be a (Disaster) for awhile
    b. Mitigation
        i. Could reconfigure and run without FW but would be non-compliant for PCI, spare FW, Cisco SmartNet 8x5 NBD
27. Wireless link to CHST
    a. Risk
        i. Loss would be no network access for CHST center
    b. Mitigation
        i. Support through Motorola
28. Mitchellcc.edu
    a. Risk
        i. Total loss would mean no access to main website, insider website, and the links students use to get to WA, Moodle, and Gmail
    b. Mitigation

i. Cloud based solution with near bullet proof survivability, as far as we know

29. Packateer
    a. Risk
        i. Loss would mean no packet shaping which could leave us open to users downloading coyrighted material
    b. Mitigation
        i. In the event of a total failure the unit will act as a passthrough
30. Einstein
    a. Risk
        i. Loss would mean no DNS, DHCP, or authentication for CEC and WFT
    b. Mitigation
        i. Network tasks could be reassigned to other network servers
31. Equinox
    a. Risk
        i. Loss would mean no DNS, DHCP, or authentication for MRSVL center
    b. Mitigation
        i. Network tasks could be reassigned to other network servers
32. NCIH
    a. Risk
        i. Loss of video which could cancel classes and meetings. If the NCIH router goes down we lose internet
    b. Mitigation
        i. MCNC SLA
33. BES
    a. Risk
        i. Loss would mean no mail to Blackberries, bigger threat is from lost devices
    b. Mitigation
        i. None
34. E-Procurement
    a. Risk
        i. Total loss means we can't make pruchases
    b. Mitigation
        i. Backups, VM
35. Gmail
    a. Risk
        i. Loss of student email and backup to Exchange
    b. Mitigation
        i. Cloud based solution with near bullet proof survivability, as far as we know
36. PRI's

a. Risk

i. Loss means we could make or receive calls outside of campus total failure is not as significant as a total Call Manager failure (internal calls would still work) but downtime of more than a couple of days would impact college operations.

b. Mitigation

i. SLA with Windstream

37. FA/Link
   a. Risk
      i. Loss means cannot access FA to buy books
   b. Mitigation
      i. Support agreement with TrimData
38. Remote location L3 switches
   a. Risk
      i. Complete loss of network access at remote locations
   b. Mitigation
      i. SmartNet 8x5 NBD and spare switches
39. AIG
   a. Risk
      i. Loss of ability to print from Datatel not as critical as datatel but downtime of more than a few days will significantly impact college operations.
   b. Mitigation
      i. Support from AIG, backups
40. 3rd floor printer MB
   a. Risk
      i. Total loss would prevent check writing
   b. Mitigation
      i. I believe we can still create manual checks if we have to
41. Stu Srv printer
   a. Risk
      i. Total loss would keep us from printing transcripts
   b. Mitigation
      i. I think we can redirect jobs to a different printer
42. Main Building fiber junctions
   a. Risk
      i. If the Main Building burns down and takes out our fiber backbone we will have no network (Total Disaster) Total loss of more than a couple days would be disaster.
      ii. We would be forced to string fiber across the circle to try and get a network back
43. LRC fiber junctions

   a. Risk
      i. If the LRC burns down and takes out the fiber connections we lose internet, datatel, remote campuses, the blade enclosure, email, pretty much everything but phones (Total Disaster)

44. LRC to MB fiber line
   a. Risk
      i. If this fiber is cut somehow we lose internet, datatel, remote campuses, the blade enclosure, email, pretty much everything but phones (Total Disaster)
   b. Mitigation
      i. We would have to get a new cable run on an emergency basis

45. VB to SB fiber
   a. Risk
      i. Loss would take out all of VB, Kirkman, and Music House

46. WFT to CEC fiber
   a. Risk
      i. Loss would take out CEC and CHST

47. Old to New Bldg MRSVL
   a. Risk
      i. Lose new building

Identify and rank critical assets for recovery prioritization

Rank	Asset	Reason
1	Network Core	Loss takes out everything
2	Fiber link LRC to MB	Loss takes out almost everything but phones
3	Datatel	Loss takes out almost all administrative, student, and financials
4	Blade Enclosure	Loss takes out several critical servers
5	Datcore	Loss takes out all datatel access when old UI is gone
6	Moodle	Loss takes out all DL classes
7	Exchange	No E-Mail
8	Phone System	No phones
9	Border FW	No internet
10	Hershey	No transcripts, purchasing, HR, etc.
11	Web Adviser	Loss would cripple registration
12	E-Commerce	Loss would cripple registration

		payments
13	Informer	Loss would severly limit Datatel functionality
14	AIG	Loss of printing ability from Datatel
15	Booklog	Loss would cripple Bookstore but only a major problem first 2 weeks of the semester
16	Unix FW	Loss stops Datatel access
17	E-Procurement	Loss stops purchasing
18	Remote L3 switches	Loss of network access at remote locations
19	Donor2	Loss would cripple endowment
20	FA/Link	Loss of ability to use FA to buy books only a major problem first 2 weeks of semester
21	Printing	Total failure would be very bad but we have numerous printers and can redirect print jobs

Disaster Risks and Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk.

Classification	Risk	Preventive Measure(s)
Physical Security	**Fire**	Smoke Detectors
		Fire Alarm
		Fire extinquishers
		No smoking policy
		Fireproof media containers
	Lightning	Proper grounding
		Power conditioning/protection
	Environment	Temp Control (AC)
		Separate AC for computer room
		Temperature monitoring
	Water	Computer room safe from water
	Electricity	Clean electricity supply
		Emergency generator
		UPS
		Emergency Lighting
	Intruder	Computer Room locked/secure
		Windows locked
		Network connections secure
		Campus Security
Technical Security	**Accessibility**	Password authentication
		Password length requirements
		Firewall
		Intrusion Detection Software
		Password uniqueness
		Router ports blocked
		Encryption/Secure Server Apps.
	Infrastructure	Cable protection/conduit
	Equipment Failure	Systems Maintenance Plans
		Redundancy
		Periodic testing
	Viral infections	Virus protection software

		Anti-spam software
		Backup systems/procedures
		Activity Logs

Risk Prevention and Information Security Policies

General

- A fire extinguisher rated for electrical fires shall be maintained in the computer room.
- An Un-interruptible Power System capable of providing 30 minutes of power to the computer will be maintained. During this 30 minute period, the administrative computer staff will attempt to shutdown suspended user processes in an orderly fashion that will prevent damage to the logical data structure.
- The UPS will be tested monthly. The test will consist of reviewing the display status of the UPS systems and ensuring that loads are within tolerance to allow acceptable backup time, and to ensure batteries are charging.
- A 50kva natural gas powered generator will be maintained for the LRC and the Main Building. These generators will insure electrical power for critical systems: Cisco Phone System, Blackboard, Datatel, IIPS, AIG, E-Mail, and Authentication Servers.
- The main computer system will be maintained via a maintenance contract. The current maintenance contract is held by Alphanumeric/SUN for the Datatel server. Various peripheral equipment will be maintained as determined best by the Director of Institutional Technology.
- Support for critical phone and networking equipment will be provided through SmartNet agreements with Cisco Systems.
- User departments are responsible for maintaining adequate training in the use of the application software. The Institutional Technology department will assist as needed to maintain as low a risk as possible for operational error. User access rights will be maintained at a minimum level.
- The Institutional Technology department shall include any appropriate features to enhance the ability of locally developed software to withstand operator error. Appropriate software development practices shall be used to minimize software failure.

- Appropriate system security shall be maintained. Practices common to the data processes industry and as recommended by NCCCS, NC ITS, and audit teams shall be adopted as possible.

- It is the practice of MCC not to modify standard administrative software as delivered by the MIS division of NCCCSO for Colleague applications, including associated UNIX configurations – without specific guidance from the system office or state auditor. Non-financial related software may be enhanced under exceptional circumstances and vendor provided security patches are applied as directed by NCCCSO.

Administrative Computing System Access and User Rights

Requests for access to application(s)/data on the administrative computing systems are submitted using an access request form. This form details the access being requested and security permissions required. The completed access request form is submitted for approval to the application area supervisor as lITed below. The approved request is submitted to the IT department and serves as the documented basis for granting user access to portions of the administrative system(s).

The application areas and the respective application supervisors are:

Financial records CC.GL, CC.AR, CC.AP, CC.PI, CC.PY, CC.EQ, CC.COMMON, CF modules	VP for Finance and Administration, Richard Lefevre and/or Director of Financial Services, Bobby Barbara Wheeler
Curriculum student records CC.RG, ST Registration Records:	Dean of Student Services, Dan Manning, and/or Director of Admissions/Registrar, Kirby Moore
CC.AD, ST Admissions Records,	Dean of Student Services Dan Manning, and/or Director of Admissions/Registrar, Kirby Moore
Continuing Education student records CC.CE, CC.LI, ST Continuing Education Student records	Vice President of Continuing Education, Carol Johnson and/or Computer Operator Cindy Wagner:
Financial Aid records CC.FA, ST Financial Aid Records	Dean of Student Services Dan Manning, and/or Director of Financial Aid, Candace Cooper
Human Resources HR module	Director of Human Resources, Jodee Fulton, and/or Lee Jan Waddell
Development Office	Director of Development, Harry Stillerman
Faculty Information, CCL, ST Faculty Information Records	Vice President for Instruction Dr. Tim Brewer
Library	Director, Learning Resources Center: Vicki Caldwell

- The system administrator will set the access rights at the lowest level for the user to perform the prescribed job functions. This same procedure will be used to provide access to the CIS (Datatel) system.

- All additions and changes of users and user rights must be authorized in writing by the application area supervisor. Documentation is on file in hardcopy, by authorizing email, or signed blanket approval.

- The IT Department will be informed by the HR office when an employee is terminated. This may be accomplished by an exit form initialed by the IT staff and signed by the Director, IT. The system access of that employee will be terminated.

- Supervisors shall inform the Director of IT immediately upon termination of an employee under unfavorable conditions. IT will immediately remove any system access for the terminated employee.

This section discusses technical contingency planning considerations for the specific types of IT systems in use by MCC. The technical considerations and solutions addressed in this section include preventive measures currently in practice as well as strategic recovery measures. The following IT platforms are addressed in this section:

- Desktop Computers and Portable Systems
- Servers
- Web Sites
- Local Area Networks
- Wide Area Networks

Several of these contingency measures are common to all IT systems. Common considerations include the following:

- Frequency of backup and offsite storage of data, applications, and the operating system
- Redundancy of critical system components or capabilities
- Documentation of system configurations and requirements .
- Interoperability between system components and between primary and alternate site equipment to expedite system recovery.
- Appropriately sized and configured power management systems and environmental controls.

i. DESKTOP COMPUTERS AND PORTABLE SYSTEMS

A desktop computer or portable system (e.g., laptop or handheld device) typically consist of a central processing unit (CPU), memory, disk storage, and various input and output devices. A PC is designed for use by one person at a time. PCs are ubiquitous in most organizations' IT infrastructures. Because the desktop and portable computers are the most common platform for routine automated processes, they are important elements in our contingency plan. PCs can be physically connected to an organization's LAN or can act as a stand-alone system.

Contingency Considerations

Contingency considerations for desktop and portable systems emphasize data availability, confidentiality, and integrity. To address these requirements, MCC has implemented the following practices:

Workstation backup procedures: Users are responsible for backing up their documents to their network folders which are backed up during normal nightly backups.

Loaner PC: IT maintains five PC's that are preconfigured with standard MCC applications that can be loaned to a user in the event of total failure of their system.

Provide Guidance on Saving Data on Personal Computers. Users are instructed to save data to a particular folder which eases the IT department's desktop support requirements. If a machine must be rebuilt, the technician will know which folders to copy and preserve while the system is being reloaded.

Standardize Hardware, Software, and Peripherals. System recovery is faster if hardware, software, and peripherals are standardized throughout the organization. MCC has standardized workstations by centralizing purchases through the IT department. Workstations are Dell, network approved workstations. Additionally, critical hardware components that would need to be recovered immediately in the event of a disaster should be compatible with off-the-shelf computer components. This compatibility will avoid delays in ordering custom-built equipment from a vendor.

ii. SERVERS

Servers support file sharing and storage, data processing, central application hosting (such as e-mail or a central database), printing, access control, user authentication, remote access connectivity, phone service, and other shared network services. Local users log into the server through networked PCs to access resources that the server provides.

Contingency Considerations

Because servers support or host numerous critical applications, server loss could cause significant problems to critical College processes. To address server vulnerabilities, the following practices have been implemented:

Store Backup Media and Software Offsite. As described previously, backup media and software are stored offsite in a secure facility. The storage facility is located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event. Specific backup procedures are documented elsewhere in this plan.

Standardize Hardware, Software, and Peripherals. System recovery is generally expedited if hardware, software, and peripherals are standardized throughout the College. MCC has standardized primary campus servers as follows:

- Administrative Systems: Sun/Oracle
- Primary Domain Controllers: Dell
- Application and file storage servers: Dell
- Groupwise email: Dell
- Phones: Cisco

Primary campus servers are generally configured with the highest level of RAID possible, within budgetary constraints. When possible servers are configured on virtual machines to allow immediate recovery of a failed sysem.

iii. WEB SITES

Web sites present information to the public or authorized personnel via the World Wide Web (Web) or a private intranet. MCC maintains the following domains for internal or external web site support:

- www.mitchellcc.edu
- www.mitchellccmail.com

Contingency Considerations

In addition to the information presented in the section on Servers, several factors were considered when determining the Web site recovery strategy. Practices for Web site contingency planning included the following measures:

Document Web Site. The MCC websites are hosted off site through application service providers. Maintenance and backup are provided by the vendor.

Web Site Programming. Web site programming is handled internally by the web master. Programming of the mitchellcc.edu web site is down through dreamweaver, the mithcellccmail.com web site programming is through the vendor supplied interface.

Coordinate Contingency Solutions with Incident Response Procedures. Because an external Web site provides an image of the organization to the public, the organization's public image could be damaged if the Web site were defaced or taken down by a cyber attack. To reduce the consequences of such an attack, communications are coordinated closely with the Public Relations office. Any incident would be reported immediately to the Webmaster who would take immediate action to disable the offending page/pages until Public Relations could be notified and site corrections could be implemented.

Web Site Maintenance Security Ability to modify web page content is closely monitored and access permissions are maintained to provide for sufficient control of website content. The website navigational structure mirrors that College's organizational structure, and as such, access permissions are granted only to authorized department personnel as approved by the supervisor of the department to identified content coordinators. Authoring permissions only are provided on a per user basis to these content coordinators according to this approved structure. Content coordinators are only able to access their approved sub webs. Access permissions are maintained on file in the IT department and web masters office. Web administration security levels access to website navigational structures, page templates, style sheets, and main site pages are granted only by the Director of IT or web master.

iv. LOCAL AREA NETWORK (LAN)

A LAN is owned by a single organization; it can be as small as two PCs attached to a single hub, or it may support hundreds of users and multiple servers. MCC campus network is organized around a Star topology with a fiber-optic infrastructure. The network is a client-server Ethernet LAN.

Contingency Considerations

The LAN recovery strategy follows the information presented earlier regarding desktops, servers, and Web sites. In addition, the following practices have been implemented:

LAN Documentation. The physical and logical LAN are available but not included with this document.

System Configuration and Vendor Information Documentation. The MCC Campus Network is based on redundant Cisco hardware. This room is physically secure and has an alarm system in place to provide security after hours. Remote campus core networks are built around Cisco hardware using layer 3. These switches are maintained in locked closets.

v. Wide Area Network (WAN)

A wide area network (WAN) is a data communications network that consists of two or more LANs that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable one LAN to interact with other LANs.

The topology for MCC's wide area network is documented on the Campus Network Diagram.

Contingency Considerations

Service Level Agreement SLA is provided by MCNC. In addition, MCC complies with governing policies set forth by State Telecommunications that govern the acceptable use of this connection.

Standardize Hardware, Software and Peripherals Hardware devices are standardized to be Cisco routers and switches.

Administrative Computing Access Security

- Each user shall have a unique user id and password.
- The only time that users should share ids is to accomplish a required job function in an emergency. At the end of the emergency the password will be changed to a new value.
- Passwords should not be written down.
- Users should protect their password from unauthorized persons.
- The password will be changed every 60 days.
- No part of the password should consist of information that may be easily associated with the user. This includes any part of the users name and SSN or other easily accessible information about the users.
- The password shall be a minimum of six characters long and should contain alphabetic, numeric, and other characters.
- Workstations left unattended will have active password protected screen savers.
- A console log of logins shall be maintained and periodically reviewed to determine if unauthorized login attempts occur.
- A script will be run daily to check for null passwords
- A script will be run daily to check for UID’s of 0
- A script will be run daily to check locked accounts
- A banner is displayed upon connection to the Administrative Computer System, both IIPS and Datatel that warns against unauthorized use of the system.

Campus Network and Email Systems Security

- Each user shall have a unique user id and password.

- The only time that users should share ids is to accomplish required job function in an emergency. At the end of the emergency the password will be changed to a new value.

- Passwords should not be written down.

- Users should protect the password from unauthorized persons.

- The password will be changed periodically.

- No part of the password should consist of information that may be easily associated with the user. This includes any part of the users name and SSN or other easily accessible information about the users.

- The password shall be a minimum of six characters long, must begin and end in an alphabetic character, and/or contain at least one numeric character.

- A console log of logins shall be maintained and periodically reviewed to determine if unauthorized login attempts occur.

- After a set number of invalid login attempts, the account is frozen for a specific period of time before it is released automatically.

Administrative System: CIS (Datatel)

Full backups are performed daily.

Backups are done using UFSdump software on a DLT tape autoloader system. Should any other software or hardware be used, compatibility with mutual aid sites and NCCCSO must be maintained.

Backups are run automatically at night. The following morning, the backup log is reviewed by the systems administrator for errors. If no errors exist, and the backup is determined to be valid, the tape is stored. The previous day's tape is relocated to a 2nd storage area located in the Grier Science Building.

In the event of a threat to the computer room facilities, administrative computer department personnel shall remove the latest backup tape from the computer room and maintain personal possession until a secure environment can be obtained. In no case shall personnel place themselves in undue personal jeopardy to obtain the tape from the computer room.

Campus Active Directory Domain Servers

Full backups are performed daily Monday through Friday.

Backups are done using the Veritas software on a DLT tape system with a tape autoloader tray on Windows Server and on DLT tape system for Netware Server.

Backups are run automatically at night. The following morning, the backup log is reviewed by the Network Administrator for errors. If no errors exist, and the backup is determined to be valid the tape is stored. The tapes are stored in the secondary tape storage location room 300 of the Main Building.

In the event of a threat to the computer room facilities, administrative computer department personnel shall remove the latest backup tape from the computer room and maintain personal possession until a secure environment can be obtained. In no case shall personnel place themselves in undue personal jeopardy to obtain the tape from the computer room.

Desktop Workstations

In an effort to prevent viral infections of College computing resources, all desktop computers are pre-loaded with Microsoft Security Essentials software. Each time a user logs on to a workstation on the campus network, the local version of command checks the assigned server for the most up-to-date virus patterns and software versions and downloads as needed.

Campus Servers

In an effort to prevent viral infections from damaging campus server systems, all servers are maintained to run the most current virus definition files using Microsoft Security Essentials software.

Anti-spam procedures

Barracuda is used as the spam filtering and virus scanning engine for the college’s e-mail system.

Barracuda monitors all of the e-mail coming into or leaving the college.

Barracuda identifies e-mail that contains viruses and e-mail that has been sent from known sources of spam, and blocks them from our system. Individual senders can be, and have been, blacklisted or whitelisted.

Barracuda also blocks incoming emails with certain types of attachments to emails that are known to frequently carry viruses.

User Account Creation/Termination Procedures

User accounts for the Administrative Computer system are established by written request. These requests are maintained on file and indicate the type of access required and documented approval of the application area supervisor.

Employee accounts are terminated when employment is terminated. Employees complete a written exit form, including the effective date of termination of employment, which is forwarded to the IT department. This form is the basis for terminating the user accounts to the campus network, and administrative computer system. This form is signed by the Director of IT who is responsible for maintaining accounts.

Critical Applications

Detail plans for each application area for which the using department wishes to maintain operations during a computer failure are to be developed and included.

HR SYSTEMS
BUSINESS OFFICE - PAYROLL SYSTEMS
BUSINESS OFFICE – OTHER FINANCIAL SYSTEMS
STUDENT SYSTEMS
Donor2
Informacast
Plato

The emergency notification list for Information Technology is shown below. These people are to be notified as soon as possible when a service interruption has occurred.

Information Systems Technology

Person	Title	On-Campus	Cellular	Home
Jeff Benfield	Director, IT Telephony and WAN Administration	4345	437-9105	528-9759
Dustin Howell	Systems Administrator	1348	682-6972	
Scott Lail	Network Administrator	4281	288-8910	
Jeff Sherrill	Instructional Technology Coordinator	3273	288-7080	
David Ross	MyCircle, Hershey Administrator	1304		
Joyce Roseberry	GroupWise Administrator	3210		
Mark Niswonger	Institutional Technology Coordinator	3102	288-8903	

It should also be noted that a web-based reporting has been put in place to forward needed help by following the following link http://mccnet.mitchell.cc.nc.us/helpdesk/. The design of this helpdesk is such that it uses intelligent routing of cases based on category to the appropriate IT staff member.

Assessment of Disruption Procedures

Upon notification of disruption of service, the Director IT will immediately arrange to assess the extent of the damage or disruption.

A typical assessment will include activities to determine:

- the cause of the disruption
- potential for additional disruption or damage
- affected physical area and status of physical infrastructure
- status of IT equipment functionality and inventory, including items that will need to be replaced
- and, estimated time to repair services to normal operations.

Once the assessment has been made, the Director IT will take the following steps:

1. Make arrangements with necessary IT staff to initiate recovery activities.
2. If additional expenditures are required for recovery activities, seek approval from the V.P. of Administration to proceed with activities.
3. Proceed with recovery activities accordingly.
4. Provide a status update to departments affected by the disruption using the above notification list, to include an estimate of time to repair, if possible.

Interruption of Services Official Notice

The Vice President of Administration and the Director of Institutional Technology, individually or in consultation, upon determining that an interruption of computer services is having or will have serious consequences for the College will place the appropriate recovery processes of this plan into effect and will notify key contact persons in the following offices to communicate the status of services within their area. In case of very minor interruptions of service or disruptions that do not affect campus network and email facilities, the Director of Institutional Technology may elect to inform the campus community via campus-wide email.

Office	Contact Person
President's Office	Dr. Douglas Eason
Administration	Richard Lefevre
Business Office	Barbara Wheeler
Financial Aid	Candace Cooper
Advisement / Testing	Libbie Morrison
Plant Operations	Gary Johnson
Instructional Services	Dr. Tim Brewer
Student Services	Dan Manning
Admissions	Kirby Moore
Continuing Education	Carol Johnson
College Relations	Harry Stillerman
Mooresville Center	Brett Fansler
Cosmetology	Catherine Leroy

Recovery Operations

Based upon the architecture of MCC's IT resources, recovery operations can vary depending upon the nature of the disruption. Generally, interruptions of service on the MCC Campus would fall into one of the following categories:

1. Electrical service interruption
2. Telephone service interruption originating off-site
3. Telephone system hardware failure
4. Email system hardware failure
5. Core network component equipment failure
6. Server component failure
7. Telecommunications cable or fiber-optic line cut
8. Data loss or corruption due to extraneous event
9. Network logical failure
10. Network hardware failure
11. Applications failure
12. Virus attack
13. Denial of Service attack (internal or external)
14. Hacking attack

Recovery Procedures

The college has taken preventive measures as outlined above in routine contingency operations to reduce the likelihood of these kind of failures to interrupt service. Systems are backed up, infrastructure is protected to a reasonable extent, and hardware has a reasonable level of redundancy built in. In spite of these measures, systems do fail from time to time.

Upon notice of systems failure, the IT department staff will undertake immediate activities to assess the problem and implement the most expedient correction. The goal is to restore services as expeditiously as possible, using data backups and exercising equipment maintenance contracts and service level agreements as necessary to return the network, telecommunications systems, or campus central computing facilities to service. In the event of loss of data, the IT department will restore to the latest data backup level available at the time.

Using the processes outlined in this plan, the IT department will take steps to keep the campus community informed when service interruptions occur and when service is restored.

Specific information on detailed recovery plans are not included in this document.

Return to Normal Operations (Reconstitution Phase)

In the reconstitution phase, recovery activities are terminated and normal operations are restored. Once the system's are restored to the level that they can support the IT system and its normal processes, the system may be transitioned back into normal operation. Activities in this phase will be performed by MCC IT staff under the direction of the Director IT. The following major activities will occur in this phase:

- Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies are in normal operation
- Restoring system hardware, software, and/or firmware as may be the case.
- Re-establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the contingency system and uploading to the restored system
- Terminating contingency operations. Official notification to be made by the Director or Assistant Director, IT
- Notifying campus personnel that operations have been restored to normal and systems use may resume. The following offices will be notified by the IT department by telephone, who in-turn will notify others in their departments or divisions:

Office	Contact Person
President's Office	Dr. Douglas Eason
Administration	Richard Lefevre
Business Office	Barbara Wheeler
Financial Aid	Candace Cooper
Public Information	Dr. William Findt
Continuing Education	Carol Johnson
Plant Operations	Gary Johnson
Instructional Services	Dr. Tim Brewer
Student Services	Dan Manning

Admissions	Kirby Moore
Enrollment Management	Kirby Moore
Advisement / Testing	Libbie Morrison
Mooresville Center	Brett Fansler
Cosmetology	Catherine Leroy

The disaster notification list for Information Technology Services is shown below. These people are to be notified as soon as possible when disaster threatens or occurs.

Safety Personnel

Person	Title	On-Campus	Cellular	Home
Gary Johnson	Executive Director of Facilities	1684		
Richard Lefevre	V.P. Finance & Administration	3217		
David Heinmiller	Director of Safety & Security	5444		

Administration

Person	Title	On-Campus
Dr. Douglas Eason	President	3205
Richard Lefevre	V.P. for Finance & Administration	3217
Dan Manning	Student Services	3281
Dr. Tim Brewer	V.P. Instruction	3264
Carol Johnson	V.P. Continuing Education	3225

Damage Assessment Procedures

Upon notification of disruption of service, the Director of Institutional Technology will immediately arrange to assess the extent of the damage or disruption.

A typical assessment will include activities to determine:

- the cause of the disruption
- potential for additional disruption or damage
- affected physical area and status of physical infrastructure
- status of IT equipment functionality and inventory, including items that will need to be replaced
- and, estimated time to repair services to normal operations.

Once the assessment has been made, the Director IT will take the following steps:

1. Make arrangements with necessary IT staff to initiate recovery activities.
2. If additional expenditures are required for recovery activities, seek approval from the V.P. Administration to proceed with activities.
3. Proceed with recovery activities accordingly.
4. Provide a status update to departments affected by the disruption using the above notification list, to include an estimate of time to repair, if possible.

Declaration of Emergency/Disaster

The Vice President of Administration, the Director Information Technologies or the Assistant Director, Information Technologies (in the Director's absence), individually or in consultation, upon determining that an interruption of computer services is having or will have serious consequences for the College will place the appropriate recovery processes of this plan into effect and will notify key contact persons in the following offices to communicate the status of services within their area.

Office	Contact Person
President's Office	Dr. Douglas Eason
Administrative Services	Richard Lefevre
Business Office	Barbara Wheeler
Financial Aid	Candace Cooper
Advisement / Testing	Libbie Morrison
Continuing Education	Carol Johnson
Facilities and Maintenance	Gary Johnson
Instructional Services	Dr. Tim Brewer
Student Services	Dan Manning
Admissions	Kirby Moore
Enrollment Management	Kirby Moore
Public Relations	Harry Stillerman
Mooresville Center	Brett Fansler

Appendices:

1. Password Reset Procedure
2. Computer and Network usage guidelines
3. Daily Check Sheet
4. Deep Freeze procedure
5. Procedures in case of hacking incident
6. Surplus Equipment procedures
7. Switch change request procedure
8. Firewall change procedure

In order to better secure the network and prevent unauthorized access we instituted a challenge response process for password reset requests some time ago. We are requesting that if you; don't remember your question and answer or, if you have never submitted a question and answer that you do so as soon as possible. The procedure for password resets is as follows:

If you need your: Voyager, Datatel, MCCNET, GroupWise, Blackboard, or Voicemail password reset, for whatever reason, you will be asked the question you have selected from the four below. Assuming you correctly answer the question your password will be reset, if you cannot correctly answer the question, or you do not have a question and answer on file, you will be required to come to MB307 with your supervisor so that we can verify your identity before resetting the password.

Please select one of the four questions below and send the number of the question you select and the answer to the question, to the IT Department by responding to this e-mail as soon as possible. To insure security we can only accept responses that are sent in the form of a reply to this e-mail.

We apologize for any inconvenience this causes but it is essential we do this to protect our systems, data, and you from unauthorized system access. If you have any questions or comments please do not hesitate to contact either Jeff Benfield at ext 4345, Marie Prather at ext 3213, or David Armstrong at ext 4281.

1) What is your pet's name?

2) What is your favorite color?

3) What county were you born in?

4) What is your mother's maiden name?

Jeffrey C Benfield
Director of Institutional Technology
Mitchell Community College

Richard Lefevre
VP for Finance & Administration
Mitchell Community College

Computer and Network Usage

POLICY

User Responsibility

Each authorized user of the college administrative computing systems, electronic mail, and/or other network services must recognize his/her responsibility in having access to technologies provided by Mitchell Community College. The user is ultimately responsible for his/her own actions. The use of computer and network technology is a privilege not a right. **This privilege may be temporarily or permanently revoked for irresponsible conduct such as violating accepted security practices, intentionally altering or deleting data that belongs to others, placing unlawful information on a system, using objectionable language, intentionally sending messages that could result in the loss of the recipient's work or systems, and intentionally interfering with the work of others by actions that hamper network performance.**

Copyright

Transferring copyrighted materials to or from the network without the express consent of the owner may be a violation of Federal Law and **may be felony under State Law. Examples of copyrighted materials are: 1.) Printed materials, books or excerpts, magazine articles, research papers, etc. 2.) Copyrighted images to include both photographs and drawings. 3.) Software that is not licensed to the college. 4.) Music or video files.**

Privacy

Electronic mail, information passing over the college's network and information stored in individual user directories are considered private and confidential **but there is no guarantee of such**. Although information must be accessed for the purpose of backup, network management, etc., the content of files or messages will not be viewed or altered without permission of the user except as follows:

1.) There is reason to believe that the account has been breached or used by someone other that the authorized user. 2.) There has bee a complaint that the account has been used for unauthorized access to another network. 3.) There is reason to believe the account is being used in violation of school policy, federal, or state law.

Harassment

Use of electronic mail or other network communication facilities to harass, offend, or annoy others is forbidden. Chain letters (Ponzi Schemes) are not just an annoyance; they are illegal (US Criminal Code, 18 USC 1341-1346)

Misuse

In the realization that the Mitchell Community College network affects not only MCC, but also the world, it is necessary that users of MCCNET do not "SPAM" or cross-post messages to various news groups or message boards. **SPAM can include but is not limited to: bulk mailings for non-college business, forwarding of chain letters, forwarding of non-college items for example jokes, cute stories, thought of the day, etc. Sending SPAM will slow network performance for all and it results in a loss of productivity for those receiving the mail.**

Password

Passwords are used as means of securing all of the various types of network accounts in use at the college. Examples of accounts where passwords are used are as follows: MCCNET network account, GroupWise, IIPS (PIOpen), Colleague, Blackboard, Voyager Learning Resource Center automated card catalog, and administrative accounts. The Institutional Technology (IT) Department will assign initial passwords for the various accounts to you, these are non-secure passwords and you are required to change them as soon as possible. Guidelines for password selection, security, and maintenance are available from the IT Department. It is the user's responsibility to protect his/her account by not knowingly allowing any person to use his/her password or share his/her account information. Procedures for requests for passwords or account creation are defined in local IT procedures and are available on the MCCNET intranet web page or by request to the IT Department. If you suspect your password has been intercepted or that your account has been breached please notify the IT Department immediately for investigation.

Security

It is the responsibility of every technology user at Mitchell Community College to protect the security of the college's technology and data assets. Many of the security breaches seen in technology today are caused by file attachments that carry either virus or Trojan Horse programs with the user unaware of the infection, for this reason we have installed Norton Anti-Virus on all PC's and servers at the college. This software is administered and updated remotely by the IT Department, without prior written approval of the Director of IT users will not disable their anti-virus software for any reason. Guidelines on how to protect yourself and your equipment are available from the IT Department. Intentional attempts to circumvent system security, guess or obtain passwords, or in any way gain unauthorized access to local or network resources (hacking) is forbidden and will result in suspension of network privileges and possibly prosecution.

Equipment

Each user is to take proper care of the college's computer or technology equipment. **Any malfunction should be reported to the Institutional Technology Department either at ext 3210**

or via e-mail to helpdesk@mitchell.cc.nc.us. Users should not attempt to move, repair, reconfigure, modify or attach external devices to the system.

Games

Users should not play games or engage in other recreational activities on college equipment and networks.

Internet

Internet access is provided on college computers and intended for authorized college business in support of the learning process. Intentionally accessing sites that contain objectionable content for example; pornography, hate speech, or gambling is not authorized on college computers.

IT Procedure: PC's going to surplus

When it is determined that a PC is no longer useable by the college and should go to surplus the following procedures will be followed:

1. Any information on PC that needs to be saved will be transferred to the network.
2. Asset tag number and former location will be transmitted to Tammy Rackley in Financial Services for update of inventory.
3. DBAN software will be run on PC to remove all information from the system's hard drive. In the event that a PC is no longer operable so that DBAN cannot be run the hard drive will be removed and destroyed to prevent accidental data compromise.
4. Machine will be removed from the Audit Wizard database.
5. Arrangements will be made with Tammy Rackley and maintenance staff to have machine transferred to storage area for eventual surplus.

Jeffrey C Benfield
Director of Institutional Technology
Mitchell Community College

Richard Lefevre
Vice President for Finance and Administration
Mitchell Community College

Reviewed May 11, 2007

Mitchell Community College
Switch/Router Change Procedure

Due to the high level of integration in our network it is essential that any changes to switch or router configurations be carefully considered before implementation and be thoroughly documented after implementation. With this in mind the following procedure will be followed for any switch/router configuration changes:

1. When a technician determines that a configuration change needs to be made to our equipment they will fill out items 1-4 on Mitchell Community College Switch/Router Configuration Change Request form.
2. Route the form to the Director of Institutional Technology for approval. If the changes are approved the Director will make the appropriate changes to the running configuration, test to insure there are no unforeseen problems with the change, if there are no problems save the change to flash, make a copy of the updated configuration and store it on \\enterprise\Info Tech\Backup Cisco Configs in the appropriate folder. The Director will also complete items 5-7 on Mitchell Community College Switch/Router Configuration Change Request form.
3. Once the change is documented and complete the requesting technician will place an updated label on the switch and complete item 8 on Mitchell Community College Switch/Router Configuration Change Request form.
4. In the event the Director of Institutional Technology is unavailable the Change Request will be sent to the Vice President of Finance and Administration for approval. If approved the Network Administrator will perform and document the change.
5. When the all items are complete and the change request form is complete it will filed with the appropriate switch or router configuration guide.

Jeffrey C Benfield
Director of Institutional Technology
Mitchell Community College

Richard Lefevre
Vice President for Finance and Administration
Mitchell Community College

Return to Normal Operations (Reconstitution Phase)

In the reconstitution phase, recovery activities are terminated and normal operations are restored. Once the system's are restored to the level that they can support the IT system and its normal processes, the system may be transitioned back into normal operation. Activities in this phase will be performed by MCC IT staff under the direction of the Director of Institutional Technology. The following major activities will occur in this phase:

- Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies are in normal operation
- Restoring system hardware, software, and/or firmware as may be the case.
- Re-establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the contingency system and uploading to the restored system
- Terminating contingency operations. Official notification to be made by the Director or Assistant Director, IT
- Notifying campus personnel that operations have been restored to normal and systems use may resume. The following offices will be notified by the IT department by telephone, who in-turn will notify others in their departments or divisions:

Office	Contact Person
President's Office	Dr. Douglas Eason
Finance and Administration	Richard Lefevre
Financial Services Office	Barbara Wheeler
Financial Aid	Candace Cooper
Public Information	Dr. William Findt
Continuing Education	Carol Johnson
Plant Operations	Gary Johnson
Instructional Services	Dr. Tim Brewer

Student Services	Dan Manning
Admissions/Registrar	Brenda Sawyer
Advisement / Testing	Donavon Kirby

Introduction

This portion of the document is a disaster recovery plan for Mitchell Community College. The information present in this plan guides College management and technical staff in the recovery of computing and network facilities operated by IT in the event that a catastrophic disaster destroys all or part of the Information Systems facilities at 500 West Board Street, Statesville, NC. The primary focus of this part of the plan is to provide an orderly way to respond to a major disaster that destroys or severely impacts the central administrative computer systems and/or campus network operated by the Institutional Technology Department. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

The following objectives have been established for the disaster recovery plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Notification/Activation phase*** to detect and assess damage and to activate the plan
  - ***Recovery phase*** to restore temporary IT operations and recover damage done to the original system
  - ***Reconstitution phase*** to restore IT system processing capabilities to normal operations.

- Identify the activities, resources, and procedures needed to carry out processing requirements during prolonged interruptions to normal operations.

- Assign responsibilities to designated personnel and provide guidance for recovering and continuing operations during prolonged periods of interruption to normal operations.

- Ensure coordination with other *MCC* staff who will participate in the contingency planning strategies.

- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Assumptions

The following assumptions were used when developing the Disaster Recovery Plan

- Catastrophic long-term disasters in which the College ceases to function for an extended period cannot be planned for. Computer services recovery from such an event will be part of a general recovery process.

- Some risks are acceptable. The College does not possess the necessary resources (financial and personnel) to protect itself against every conceivable risk.

- The campus network or critical server is inoperable at the MCC campus and cannot likely be recovered within *72 hours*.

- Critical Systems/Applications are affected.

- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Disaster Recovery Plan.

- Preventive controls (e.g., generators, environmental controls, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.

- Computer center equipment, including components supporting the campus network or critical server are connected to an uninterruptible power supply (UPS) that provides *30 minutes to 1 hour* of electricity during a power failure.

- The campus network or critical server hardware and software at the MCC campus are expected to be unavailable for at least *72 hours*.

- Current backups of the application software and data are intact and available at the offsite storage facility.

- The equipment, connections, and capabilities required to operate are proposed to available at NCCCSO via a hot-site.

- Service agreements are maintained with hardware, software, and communications providers that service the College to support the emergency system recovery.

Damage Assessment Procedures
Upon notification of disruption of service, the Director of Institutional Technology will immediately arrange to assess the extent of the damage or disruption.

A typical assessment will include activities to determine:

- the cause of the disruption
- potential for additional disruption or damage
- affected physical area and status of physical infrastructure
- status of IT equipment functionality and inventory, including items that will need to be replaced
- and, estimated time to repair services to normal operations.

Once the assessment has been made, the Director of Institutional Technology will take the following steps:

5. Make arrangements with necessary IT staff to initiate recovery activities.
6. If additional expenditures are required for recovery activities, seek approval from the V.P. for Finance and Administration to proceed with activities.
7. Proceed with recovery activities accordingly.
8. Provide a status update to departments affected by the disruption using the above notification list, to include an estimate of time to repair, if possible.

Declaration of Emergency/Disaster

The Vice President for Finance and Administration and the Director of Institutional Technologies individually or in consultation, upon determining that an interruption of computer services is having or will have serious consequences for the College will place the appropriate recovery processes of this plan into effect and will notify key contact persons in the following offices to communicate the status of services within their area.

Office	Contact Person
President's Office	Dr. Douglas Eason
Finance and Administration	Richard Lefevre
Financial Services Office	Barbara Wheeler
Financial Aid	Candace Copper
Advisement / Testing	Donavon Kirby
Continuing Education	Carol Johnson
Plant Operations	Gary Johnson
Curriculum Instruction	Dr. Tim Brewer
Student Services	Dan Manning
Admissions/Registrar	Kirby Moore
Public Relations	Harry Stillerman

Disaster Recovery Preparations

The Systems Administrator, Institutional Technology, will maintain backup copies of all software and data. The backups will be maintained to ensure availability in the event of an emergency or disaster. Specific backup procedures are documented in this plan. The College will maintain mutual aid agreements with one or more compatible sites at which essential operations can be performed. The Director of Institutional Technology shall coordinate with the system management personnel of the mutual aid sites for implementing the use of the site.

An individual plan for each department responsible for critical applications shall be maintained. The plan shall address actions to be taken if an emergency or disaster interrupted computer availability. The plan should consider the maximum time that the department could operate without computer support and periodic peak processing requirements. Each department should consider developing manual alternative processes to the automated computer processes and the entry of the data generated by the alternative process into the computer database. The plan should address individual items of equipment used by the department for data processing. A minimum level of capability shall be defined for each department. If the department is to continue limited operation at the mutual aid site, then the department plan should address how this is to be accomplished. The Director of Institutional Technology will assist each department in the development of the individual department plan. Departmental plans are contained in this document for those responsible for critical applications.

The College will maintain adequate insurance coverage to replace or repair the computer system in the event damages are caused to the computer systems that are not covered by a service agreement. Sources of replacement equipment will be maintained. This plan contains a list of primary equipment and replacement sources.

Recovery Operations

Based upon the architecture of MCC's IT resources, recovery operations can vary depending upon the nature of the damage. Generally, disasters relating to IT services on the MCC Campus would fall into one of the following categories:

1. IT central computer room facilities located in Main building are destroyed all or in part.
2. IT core network facilities Main, LRC, Vocational Building, Science Building and Continuing Educational Center building are destroyed all or in part.
3. Core network facilities at the remote campuses, Mooresville Center is destroyed all or in part.

4. Campus network communications facilities are lost to any other particular building on campus, but are confined to locations not affecting the core network equipment or central campus server farm.
5. All facilities are destroyed, resulting in a general campus shutdown.

Recovery Procedures

1. *IT central computer room facilities located in Main building are destroyed all or in part.*

In this case, telecommunications facilities would be left in tact, with the possible exception of facilities within Main building. This only affects a small number of handsets on campus in Main building. Staff using these handsets could make temporary alternate arrangements until restored. As an alternative, these handsets could be temporarily affected staff could use cellular phones until restored.

If the college's central computer room is destroyed administrative systems and domain control would be handled by redundant systems located in Main Building. For permanent restoration alternate servers would have to be purchased under expedited delivery, set up in Main building in the network core room, and the latest applications reloaded from backup tapes stored in the off-site location.

Once services are restored to temporary status, continue with permanent facilities replacement.

2. *IT core network facilities located in Main building are destroyed all or in part.*

In this case, network and telecommunications facilities serving a large number faculty, student services and continuing education would be destroyed including, the switchboard. This type of disaster would not be easily recovered from. Recovery would involve the following procedures:

- Relocating central office facilities to other buildings temporarily. Major planning and recovery efforts would have to be coordinated with networking and telecommunications providers.
- Networking services would be lost in Science, Vocational, or LRC buildings.
- Arrange from temporary cable splices to intercept cables outside of LRC building to restore a portion of networking service to the buildings named above on campus.
- The switchboard would have to be relocated to another building during this time.

Upon the loss of Main building, the campus computing network core would be lost in Science, Vocational, LRC buildings. This includes the fiber optic feeds that route to each building. The following procedure would restore the campus network in the shortest time possible.

- Using Cisco L3 enabled switch, establish a new, temporary core, in Main building. Contract fiber cabling vendors to reroute cabling from cable vault to aerial link into Main with priority install within 5 working days maximum.
- Reconfigure core switch to accommodate new fiber links.

Once services are restored to temporary status, continue with permanent facilities replacement.

3. *Core network or telephone facilities at Mooresville is destroyed all or in part.*

In the case of telephone or network facilities being destroyed at a remote campus site, the following recovery procedures would be performed:

- Arrange with dial-tone providers to restore communications facilities to the site, at an alternate location if necessary.
- Arrange for replacement switch equipment to be shipped overnight.
- Reinstall telecommunications equipment in original or alternate location.
- Provide temporary communications for staff using cellular phone service if necessary.
- Temporarily relocate staff and students to Main campus until remote facility becomes usable.

Once services are restored to temporary status, continue with permanent facilities replacement.

4. *Campus network or telecommunications facilities are lost to any other particular building on campus, but are confined to locations not affecting the core network equipment or central campus server farm.*

This situation would not affect the overall campus network or telecommunications facilities. In this case the following procedures would be in effect:

- Install a temporary building connection switch at the location where staff would be relocated.
- Since all buildings on campus are wired, service could be provided at any alternate site chosen on a temporary basis.

Once services are restored to temporary status, continue with permanent facilities replacement.

5. *All facilities are destroyed, resulting in a general campus shutdown.*

Catastrophic long-term disasters in which the College ceases to function for an extended period cannot be planned for. Computer services recovery from such an event will be part of a general recovery process. In this event, select applications such as payroll could be performed by use of an alternate site at the discretion of the President.

Return to Normal Operations (Reconstitution Phase)

In the reconstitution phase, recovery activities are terminated and normal operations are transferred back to MCC's computer operations facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the contingency system should continue to be operated. Activities in this phase will be performed by MCC IT staff under the direction of the Director of Institutional Technology. The following major activities will occur in this phase:

- Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies
- Installing system hardware, software, and firmware. This activity includes detailed restoration procedures similar to those followed in the Recovery Phase
- Establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the contingency system and uploading to the restored system
- Shutting down the contingency system
- Terminating contingency operations. Official notification to be made by the Director of Institutional Technology
- Notifying campus personnel that operations have been restored to normal and systems use may resume. The following offices will be notified by the IT department by telephone:

Office	Contact Person
President's Office	Dr. Douglas Eason
Finance and Administration	Richard Lefevre
Financial Services Office	Barbara Wheeler
Financial Aid	Candace Copper
Advisement / Testing	Donavon Kirby
Continuing Education	Carol Johnson
Plant Operations	Gary Johnson
Curriculum Instruction	Dr. Tim Brewer
Student Services	Dan Manning
Admissions/Registrar	Brenda Sawyer
Public Relations	Dr. William Findt

- Securing, removing, and/or relocating all sensitive materials at the contingency site
- Arranging for recovery personnel to return to the original facility.

Appendices

1. **Organizational Personnel**
2. **Vendor Contact List**
3. **Security is Everyone's Concern**
4. **Internet Acceptable Use Policy**
5. **Computer Replacement Policy**

Organizational Personnel

This organization chart includes only the key personnel required in initial response to a major emergency or disaster. Key personnel for user departments are listed in individual department plans.

Director, Institutional Technology

The Director of Institutional Technology is responsible for this plan under the direction of the Vice President for Finance and Administration. The Director of IT serves as the college information security officer.

Systems Administrator

This position provides technical and administrative support the College computer network and coordinates Netware / GroupWise related issues.

Vice President for Finance and Administration

The Vice President for Finance and Administration is responsible for general management of financial support needed to support college computing. All expenditures relating to the operation of this function and to this plan are approved by the Vice President for Finance and Administration.

Executive Director of Facilities and Auxiliary Services

Provides the general facilities maintenance for the computer operations area. In an emergency or disaster, this position will provide support as directed by the Vice President for Finance and Administration to facilitate the restoration of computing services.

Mitchell Community College

Vendor Contact List

Person	Vendor	Telephone
Ike Bunn	ENS	919-510-0510
M Hildebrandt	ENS	
	Dell Computer	800-945-3355
	Gateway	877-485-1464
	Sun	
	Alphanumeric Systems	919.781.7575
	ITS	800-722-3946
	Unix Datatel Sun 450	
	IBM IIPS F-40	800-426-7378

Mitchell Community College
IT Equipment, Manufacturer and Serial Numbers

				Date
Location	**Description**	**Manufacturer**	**Serial No.**	**SB #**
Main CR	Risc 6000 F40 (IIPS legacy server)	IBM	10-18350	008224
Main CR	Sun E450 (Colleague server)	Sun	203V0012	008929
Main CR	StorEdge L9 Tape System	Sun		
Main CR	Accelar 1100R-B Layer 3 Switch (in use)	Nortel Networks		
Main CR	Accelar 1100R-B Layer 3 Switch (spare)	Nortel Networks		008824
Main CR	2800 Series Router owned by ITS	Cisco		
Main CR	Pix Firewall	Cisco		008823
Main CR	VPN 3000 Concentrator	Cisco		009538
Main CR	IPS	Top Layer		009822
Main CR	Cisco 3700	Cisco		009270
Main CR	Spam Firewall 400	Barracuda		009644
Main CR	Fortigate 500A	Fortinet		009697
Main CR	Bay Stack 450-24T Switch	Nortel Networks		008383
Main CR	Bay Stack 450-24T Switch	Nortel Networks		008390
Main CR	Bay Stack 450-24T Switch	Nortel Networks		008381
Main CR	Bay Stack 450-24T Switch	Nortel Networks		008382
Main CR	Bay Stack 450-24T Switch	Nortel Networks		008561
Main CR	Poweredge 2650 aig-archives	Dell		009652
Main CR	Poweredge 2650 webadvisor	Dell		009653
Main CR	Poweredge 2650 pserver	Dell		009654
Main CR	Poweredge 2650 MCC_bb6	Dell		009392
Main CR	Poweredge 2650 MCC_vir_domain	Dell		009597
Main CR	Poweredge 2650 dhcp-dns2	Dell		009596
Main CR	Poweredge 2650 MCC_proxy	Dell		009595
Main CR	PowerVault 132T Tape backup	Dell		009656
Main CR	PowerVault 220S Richmond Disk Array	Dell		009655
Main CR	Poweredge rack console 15FP	Dell		
Main CR	Untoview 200	Avocent		009651
Main CR	Proliant DL380	HP		009679
Main CR	Powervault 112T Tape Backup	Dell		009606
Main CR	7400 Server MCCimages	Gateway		008925
Main CR	Proliant ML530 helpdesk	Compaq/HP		008645
Main CR	10/100 Fast Ethernet switch	D-Link		
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008727
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008724
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008726
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008725
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008722
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008723
Main 032	Bay Stack 450-24T Switch	Nortel Networks		009269
Main 032	Bay Stack 450-24T Switch	Nortel Networks		009272
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008728
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008387
Main 032	Bay Stack 450-24T Switch	Nortel Networks		008388

Main 23	ENH724-DS 24 port hub	Encore	
Main 23	ENH724-DS 24 port hub	Encore	
Main 2	Aironet 1100 Wireless AP	Cisco	
LP Office	Bay Stack 450-24T Switch	Novell Networks	008563
LP Office	Bay Stack 450-24T Switch	Novell Networks	008564
LP Office	Bay Stack 450-24T Switch	Novell Networks	008565
LP Office	Bay Stack 450-24T Switch	Novell Networks	009271
LP Office	Bay Stack 450-24T Switch	Novell Networks	008384
LP Office	Bay Stack 450-24T Switch	Novell Networks	008857
LP Office	Bay Stack 450-24T Switch	Novell Networks	008562
LP			
Purcell	7400 Server lburgserv	Gateway	008720
Purcell	Bay Stack 450-24T Switch	Nortel Networks	
Purcell	1721 Router	Cisco	
Purcell	Aironet 350	Cisco	
Speller	Bay Stack 450-24T Switch	Nortel Networks	
James	Bay Stack 450-24T Switch	Nortel Networks	
James	1721 Router	Cisco	
James	10/100 Fast Ethernet switch	D-Link	
James	Airnet 350	Cisco??????	
Rockingham	Bay Stack 450-24T Switch	Nortel Networks	
Rockingham	Bay Stack 450-24T Switch	Nortel Networks	
Rockingham	1721 Router	Cisco	
Condor GSC	Aironet 1100	Cisco	
Condor 123	Aironet 350	Cisco	
Condor 130	Aironet 350	Cisco	
Condor 118	Bay Stack 450-24T Switch	Nortel Networks	008385
Condor 118	Bay Stack 450-24T Switch	Nortel Networks	008566
Condor 118	Bay Stack 450-24T Switch	Nortel Networks	008567
Forte 324	Bay Stack 450-24T Switch	Nortel Networks	008389
Main 201	Bay Stack 350T-HD	Nortel Networks	008234
Main 209	Wave Point 2 Wireless Bridge	Lucent	008380
Cole	Wave Point 2 Wireless Bridge	Lucent	008379
Cole	Link Builder FMS 2	3 Com	n/a
Grimsley	Bay Stack 450-24T Switch	Nortel Networks	n/a

Security is Everyone's Concern

MCC is a campus everyone can be proud of. From the breathtaking views to the well maintained grounds and buildings. We can also be proud of the fact that we have one of the safest colleges in the state. Everyone whether in uniform or not uses their eyes and ears to be alert to anything suspicious and then reports it to security for follow-up.

In addition to using our senses to keep the campus safe there are a number of other common sense things that can be done to both keep our campus safe and keep petty theft down. Most of the crimes that occur on campus fall into a "crimes of opportunity" category. An individual may not have come here to commit a crime but seeing a purse on a desk or on the seat of an unlocked car may be too big a temptation for some individuals.

The same is true with computers, especially lap tops. Leaving them unsecured or in the open is just too tempting for some folks. Computer labs and classrooms unfortunately are not exempt from petty theft. The new computers and towers in many instances do not need any tools to open them up and remove memory chips or other valuable components. Labs should be locked when not in use and unsupervised. Faculty/staff should "log off" from the PC in your office when you leave. This can be done from the START menu on a pc without having to shut down the workstation, and provides security against unauthorized use of your computer. We are currently evaluating other means of providing a more secure campus network such as the use of ID's/passwords for students and additional security measures that we can implement in conjunction with the state's perimeter security firewall.

We can all help prevent this by taking some simple steps. Lock all rooms and offices when we vacate them. Most of us would not think of leaving home with the door left wide open, but we do not give it a second thought when leaving our office or classroom and just leave the door opened. Men leave jackets with wallets and other valuables; women leave their purses in open unattended rooms and then go teach a class. There are some that do this and also leave their keys in the door. We all have what we perceive to be perfectly good reasons for doing this but the main reason is that we are too lazy to take the few extra seconds to secure the room. Also, please report any instances of theft or other breeches of security immediately to your supervisor.

It may seem like an inconvenience to lock the door each time you leave, even for a few moments, however "the valuables you save may be your own." Please let's all of us become more security conscious and lock unattended rooms.

Internet and Campus Network Acceptable Use Policy Date last revised February 1998

Mitchell Community College provides campus network and computing facilities including Internet access for the use of faculty, staff, students, and other authorized individuals in support of the research, educational, and administrative purposes of the College. The College has extensive information technology resources and systems available for both instruction and administrative applications. Faculty, staff, and students are encouraged to become familiar with College technology resources and systems and to use them on a regular basis.

Users are expected to exercise responsible, ethical behavior when using these resources and to adhere to the following guidelines:

1. The Internet and associated resources contain a wide variety of material and information. Information available on the Internet is not generated or selected by Mitchell Community College. The College is not responsible for the accuracy or quality of the information obtained through or stored on the campus network.

2. The creation, display, or transmittal of illegal, malicious, or obscene material is prohibited.

3. Mitchell Community College will not be liable for the actions of anyone connecting to the Internet through College facilities. All users shall assume full liability (legal, financial, or otherwise) for their actions.

4. The user is responsible for complying with laws protecting software or other accessed information. Downloading programs and files may violate United States copyright laws that protect information and software. Although the Internet provides easy access to software distributed by companies on a trial basis, this does not mean that the software is free or that it may be distributed freely. All files downloaded from a source external to the campus must be scanned for viruses.

5. Because of the unsecure nature of transmitting files electronically, no right of privacy exits with regard to E-mail, Internet sessions, or electronic file storage and transmission. When sending or forwarding E-mail over the campus network or the Internet, users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden.

6. Mitchell Community College computing and telephone facilities maintain usage statistics in archived log files for the purpose of monitoring system performance and usage patterns. Users must not perform tasks they would not want logged.

7. College employees may make reasonable personal use of the campus network, E-mail, and the Internet as long as the direct measurable cost to the public is none or is negligible, and there is no

negative impact on employee's performance of duties.

8. All users of the Internet by way of College facilities must comply with all relevant policies and procedures of the College.

9. Use of the Internet for commercial gain or profit is not allowed from a College site.

Failure to comply with any of these provisions will result in disciplinary action as provided for under the disciplinary policies and procedures of the College.

Computer Resources Replacement Policy

GENERAL STATEMENT

Mitchell Community College is committed to the support of all its educational programs and administrative processes with the latest technology available for instruction, management and information access. Through the use of technology, enhanced educational outcomes will equip students for a technology and information-driven society. Utilization of technology in all areas of College administration will help to ensure quality services, increased productivity and efficient management of state, local and college resources.

The use of computer technology resources must be consistent with the mission and goals of the College. Ail computer users are informed about the College's Acceptable Use Policy and regulations imposed by the State of North Carolina. Users, including faculty, staff, students and community patrons are required to follow the College's guidelines, policies and procedures as they access information technology and electronic networks available on the Campus. All such use is governed by and must be consistent with the regulations of Mitchell Community College, as well as local, state and federal laws.

The College receives its primary funding from the State of North Carolina. Within the parameters of existing funding sources, the College recognizes that it is impossible to guarantee that sufficient resources and funding will be available to replace computer hardware and software on a predetermined schedule. The purpose of this policy is to ensure the most efficient and equitable allocation of computer resources within the limitations of available funding.

This policy applies to all College computer and telecommunications systems. It refers to all hardware, data, software, and associated communications networks. In particular, this policy covers computers ranging from multi-user timesharing systems to single user personal computers that are connected to the College's campus-wide network.

REPLACEMENT CYCLE

Mitchell Community College recognizes the need to provide computer hardware and software resources adequate to deliver high quality, up-to-date instructional and informational services. Rapid technological changes in both hardware and software, in addition to highly sophisticated instructional methodologies, make it essential that frequent upgrading of these resources be implemented to ensure access to basic services. The replacement cycle, consistent with standard industry practice, shall be three to five years. Every effort will be made to upgrade existing equipment to the limit of hardware capability and utilization of each unit before discarding in a manner defined by State surplus property guidelines. To date, the three-to-five year cycle has been met or exceeded in all essential areas of the College.

Laws Pertaining to the Use of State Computer Systems

Federal Law:
United States Code, Title 18, Section 1030. "Fraud and related activity in connection with computers"

North Carolina Statutes: www.ncleg.net

Chapter 14. Criminal Law. Article 60. Computer-Related Crime.

§ 14-453.	**Definitions.**
§ 14-453.1.	**Exceptions.**
§ 14-453.2.	**Jurisdiction.**
§ 14-454.	**Accessing computers.**
§ 14-454.1.	**Accessing government computers.**
§ 14-455.	**Damaging computers, computer programs, computer systems, computer networks, and resources.**
§ 14-456.	**Denial of computer services to an authorized user.**
§ 14-456.1.	**Denial of government computer services to an authorized user.**
§ 14-457.	**Extortion.**
§ 14-458.	**Computer trespass; penalty.**

Mitchell Community College
Disaster Recovery Plan
Test Procedures

Mitchell Community College adopts the walk-through method of testing as the most practical means of testing disaster readiness and recovery procedures relating to the most catastrophic types of failures identified in the plan. A comprehensive walk-through is performed annually at the time the Financial Services Continuity Plan/Disaster Recovery Plan is revised. The walk-through serves as a method for identifying weaknesses in the plan as well as a method of communicating the plan to IT staff and to the rest of the campus faculty/staff. Each identified component of the disaster recovery plan has an identified testing procedure as listed in the following table:

Plan Component or Disaster Scenario	Test Methodology	2002-2003 Test Data	Results
Catastrophic Interruptions			
Category 1 disaster	Walk-through		
Category 2 disaster	Walk-through		
Category 3 disaster	Walk-through		
Category 4 disaster	Walk-through		
Category 5 disaster	Walk-through		
Other Interruptions:			
UPS testing	Non-interruptive status test; read display log		
911 emergency test	Test call to 911		
Viral Infection containment	Walk-through		
Insurance Review:	Review policy coverage with VP for Finance and		

	Administration; evaluate Financial Services interruption protection ($5,000,000)		
Plan Distribution	Technology Committee Meeting: Comprehensive BCP plan presentation and discussion		
Maintenance Contract Review	Review each contract annually at time of renewal		

Mitchell Community College
Administrative Computer Systems
User Access Definition and Account Request Form

Employee Information:

Employee's Name:

Job Title:

Department:

Supervisor's Name:

Administrative Systems Access Information:

Indicate systems access is needed for:

IIPS □ CIS (Datatel) □

For each system requested describe the systems for which access is to be approved. (Indicate screens, mnemonics, security classes, or menus as required; or, provide the name of another active employee or group with the same access level to be used as an access pattern.)

__________________________________ ____________________

Application Supervisor's signature: Date

__________________________________ ____________________

Vice-President, Administrative Services Date

The application areas and the respective application supervisors are:

Financial records CC.GL, CC.AR, CC.AP, CC.PI, CC.PY, CC.EQ, CC.COMMON, CF modules	Director of Financial Services Barbara Wheeler
Curriculum student records CC.RG, ST Registration Records:	Director of Admissions / Registrar, Brenda Sawyer
CC.AD, ST Admissions Records,	Director of Admissions / Registrar, Brenda Sawyer
Student Advising / Testing System	Director of Counseling, Donavon Kirby
Continuing Education student records CC.CE, CC.LI, ST Continuing Education Student records	Vice President for Continuing Education, Carol Johnson
Financial Aid records CC.FA, ST Financial Aid Records	Director of Financial Aid, Candace Cooper
Personnel HR module	Director, Human Resources, Jodee Fulton
Development Office	Vice President for Development / Foundation, Dr. William Findt
Bookstore CC.BI; Bookstore Inventory System	Bookstore Manager Donna Arnett
Faculty Information, CCL, ST Faculty Information Records	Vice President, Instruction: Tim Brewer
Library	Director, Learning Resources Center: Rex Klett

8.06.00 SAFETY AND HEALTH PROGRAMS

It is the consideration of top management that the employees of Mitchell Community College are our most important assets, and every effort will be made to protect them by providing a safe and healthy working place. This is the primary responsibility of each supervisor. In addition, each employee must carefully follow established safe work practices. We will voluntarily comply with both the letter and intent of safety and health standards promulgated under the Occupational Safety and Health Act of 1970. Doing so is not only a moral obligation, but is inseparable from good management of our limited and most precious resource - the employees.

A. Director of Safety, Energy Management and Security

The Director of Safety, Energy Management and Security is designated as the focal point for all matters pertaining to employee safety and health. The Director of Safety, Energy Management and Security will function in the role of coordinator and assist department heads in fulfilling their responsibilities for preventing accidents. The Director of Safety, Energy Management and Security will continuously monitor the progress of this plan to control accidental losses and keep top management informed on both the progress being made and problems that develop.

B. No Loss of Pay

The time during which employees are participating in training and education activities shall be considered as hours worked for purposes of wages, benefits, and other terms and conditions of employment. The training and education shall be provided at no cost to the employees. Members of the safety committee shall be allowed reasonable time to exercise the rights of the committee without any loss of pay or benefits for time spent on duties of the committee.

C. Self Inspection/Evaluation

The safety chair in cooperation with the safety committee will cause a thorough inspection to be made within the workplace as often as necessary, but at least once every three months. Particular attention will be given to employee work 95 habits in addition to identifying hazardous conditions. During this inspection, employees will be consulted and their concerns addressed. A written record of the inspection results and a list of corrective actions taken will be maintained by the safety chair for review. Realistic dates shall be established for correcting each hazard noted during an inspection and the safety chair will track corrections of hazards. Department heads and supervisors shall be responsible for ensuring correction of hazards in their work areas. File copies of all inspections will be retained in the workplace by the safety chair for two years.

D. Safety and Health Training For Employees and Committee Members

Supervisors should be our most knowledgeable, skillful, and safety conscious employees. Supervisors are to always set a good example for subordinates and to constantly function as their trainer. During initial orientation of current and new employees, management will ensure that the employees are fully capable of coping with all potential emergencies and are aware of job related hazards. An employee is not to work without direct, immediate supervision until this is accomplished. All employees will be provided a copy of the company safety and health policy (in the Faculty/Staff Handbook) during orientation, which shall be reviewed by the safety chair and supervisor with the employee. Safety and health committee members and supervisors will receive additional training on the company's safety and health program, hazard recognition, hazard correction and control, and the rights and responsibilities of the safety committee as outlined elsewhere in this document. Occupational safety and health refresher training will be provided for employees and committee members at least annually and when operation changes result in new or different safety or health hazards. The safety chair will facilitate all safety and health training necessary and retain all written plans necessary to maintain an ongoing effective safety and health program.

E. Emergency Situation and Medical Treatment

Emergency telephone numbers (fire, rescue, etc.) should be conspicuously posted near every telephone unit. The responses to emergency situations, which may affect all employees, will be planned and coordinated by the safety chair and safety committee.

Department heads will identify and plan courses of action for special emergencies, which would be confined to their sphere of responsibility. Emergency procedures will be exercised as often as necessary, to ensure proficiency in coping with the emergency, but no less often than once a year. First aid medical care will be provided through the Department Head, who shall have access to first-aid supplies and trained first aid medical personnel. 96

F. Accident and Illness Investigation

Personal injuries (other than first aid), property damage, accidents, "near misses" that could have resulted in personal injury, and all occupational illnesses will be promptly and thoroughly investigated to determine what happened, why it happened, and what should be done to prevent recurrence of similar mishaps or conditions. The responsible supervisor will ensure that such an investigation is conducted and will obtain technical assistance from other sources as needed. The safety chair and safety committee will review all such reports and recommend any further action necessary.

G. Other Employers/Employees on Site

The safety chair shall be responsible for ensuring that all outside employers who have employees on our site comply with our safety and health rules. Outside employers shall be required to review with the safety chair all planned work procedures and potential hazards before any work begins. The safety coordinator will in turn review this information with department heads and supervisors. Department heads and supervisors will inform and train affected employees. No outside employer will be allowed to perform work on our site if it cannot be done safely. The safety coordinator shall maintain supporting documentation of this activity.

H. General Employee Safety Rules

Managers and supervisors at all levels will strictly enforce the following general rules for employee protection.

1. Promptly report all accidents to your immediate supervisor even when an injury is not readily apparent, such as a possible strain of lower back muscles.
2. Wear the prescribed personal protective equipment for each job and ensure that it is in a fully serviceable condition before commencing work.
3. Loose clothing, jewelry, and hair longer than shoulder length shall not be worn around moving machinery.
4. Smoke only in those areas designated for smoking.
5. Employees will report to work in a rested condition, unaffected by alcohol or drugs.
6. Firearms and other types of dangerous weapons will not be brought onto the premises, except for sworn law enforcement officers.
7. Operate only those machines on which you have been trained by supervision.
8. Avoid running and all undue haste. Do not engage in horseplay or taking chances.

9. Lift objects with leg muscles and keep the load close to your body. When in doubt as to your safety, always get assistance or use a mechanical lifting device.
10. Do not take chances with any job. Pause and think before acting. If in doubt, ask your supervisor. Do not use defective equipment. Employees who knowingly violate these rules or established safe work practices will be subject to appropriate disciplinary actions as set forth in 97.

Section 8.02.00, Discipline, and Dismissal. Flagrant violations may result in termination of employment on the spot.

I. Safety and Health Committee

A safety and health committee will be part of our safety program. Half of the committee will be non-management employees and in representative numbers as described in General Statute 95-252.

1. Selection
   Employee safety and health representatives shall be selected by and from the non-managerial employees. The safety chair will facilitate the selection process of the committee members.
2. Co-Chair
   The Safety and health committee shall be co-chaired by a representative selected by the employee members of the committee.
3. Rights
   The safety and health committee shall, within reasonable limits and in a reasonable manner, exercise the following rights:
   a. Review the safety and health program established by the employer.
   b. Review incidents involving work-related fatalities, injuries and illnesses, and complaints by employees regarding safety or health hazards.
   c. Review, upon the request of the committee or upon the request of the employer representative or employee representatives of the committee, the employer's work injury and illness records, other than personally identifiable medical information, and other reports or documents relating to occupational safety and health.
   d. Conduct inspections of the worksite at least once every three months and in response to complaints by employees or committee members regarding safety or health hazards.
   e. Conduct interviews with employees in conjunction with inspections of the worksite.
   f. Conduct meetings, at least once every three months, and maintain written minutes of the meetings.
   g. Establish procedures for exercising the rights of the committee.
   h. Make recommendations on behalf of the committee, and in making recommendations, permit any members of the committee to submit separate views to top management for improving the program.

8.06.01 BLOODBORNE PATHOGENS EXPOSURE CONTROL PLAN

It is mandatory that all Mitchell Community College employees attend annual training sessions to review the College's Blood Borne Pathogens Exposure Control 98 Plan. Documentation of each employee's attendance is maintained in the Personnel Office and subject to review by the Occupational Safety and Health Administration (OSHA).

8.06.02 CHEMICAL HYGIENE PLAN AND HAZARDOUS COMMUNICATION PLAN

It is mandatory that all maintenance employees, nursing staff, and biology/chemistry instructors attend annual training sessions to review the College's Chemical Hygiene and Hazardous Communication Plans. Documentation of each employee's attendance is maintained in the Personnel

Office and subject to review by the Occupational Safety and Health Administration (OSHA). The Chemical Hygiene Officer keeps these plans.

8.06.03 PERSONAL PROTECTIVE EQUIPMENT (PPE) PROGRAM, FORKLIFT PROGRAM AND TAGOUT PROGRAM

It is mandatory that employees covered by these plans be trained as specified in each of these plans. The training logs for these programs are to be maintained by the Maintenance Engineer. The Maintenance Engineer maintains and keeps these plans.

8.07.00 SMOKING

Smoking is NOT permitted in MCC facilities. This includes all buildings on the Main Campus, Cherry Street Center, Continuing Educational Center, Cosmetology Center, Mooresville Center and the South Statesville Skills Center. This also includes all classes taught by MCC personnel, regardless of the location. Faculty and staff are asked to observe smoking regulations as a courtesy and as a safety precaution.

Smoking on campus is allowed in designated smoking areas. Ashtrays and containers have been provided in the designated outside areas to help keep the campus clean.

8.12.00 INCLEMENT WEATHER ATTENDANCE

When it is necessary to close the College due to inclement weather, disaster, etc., class time shall be made up according to the number of hours missed under the direction of the Vice President of Instruction.

Other weather interruptions will be handled by policy on "make-up" i.e., documented within the semester by extra class time or extra assignments. Faculty and/or staff will be required to make up the time if the classes are scheduled on a traditional non-work day (Saturday or a holiday). Example: If classes are made up on a day the College was scheduled to be closed (i.e. Good Friday) then all employees must work. If the classes are made up by extra assignments, etc. neither faculty nor staff will make up the time.

The President will determine when and how the classes will be made up. In the event of extra assignments, each individual faculty will document and note on their official class roster their own make up and the documentation will be presented to the Vice President of Instruction within two days of the made up assignment. Faculty, staff, and students will be notified by the following radio and television stations of the weather-delay schedule. Those stations are:

WAME—550 AM
WBT—1110 AM WBT—99.3 FM
WSIC—1400 AM
WHIP—1350 AM
WIBT—96.1 FM
WKKT—96.9 FM
WRFK—99.7 FM

WLYT—Lite 102.9 FM
Wend—106.5 FM
The Link—107.9 FM
WBTV (CBS)—TV Channel 3
WSOC (ABC)—TV Channel 9
WCNC (NBC)—TV Channel 36/Cable 6
WXII (NBC)—TV Channel 12

Visit our webpage at http://www.mitchellcc.edu/

IF THERE IS NO ANNOUNCEMENT, THE COLLEGE WILL BE IN OPERATION AS USUAL.

8.13.00 EMERGENCY PLAN

A. General

1. This plan outlines procedures for reacting to fires, bomb threats, or other emergency situations in Mitchell Community College facilities located on the Main Campus.
2. Emergency plans for other college buildings will be prepared and maintained as follows:

Building Responsible Staff Member

Historic Campus—Vice President for Finance and Administration
Continuing Education Center—Vice President for Continuing Education
Mooresville Center—Director of the Mooresville Center
Cherry Street Center—Director of Safety, Energy Management and Security
South Statesville Skills Center—Director of South Statesville Skills Center
Cosmetology Center—Cosmetology Program Director

3. The Dean of Instructional Services has the overall responsibility for this plan, its implementation, and any required changes.

B. Responsibilities

1. In the event of an emergency, the administrator in charge, assisted by the building marshals, is responsible for the implementation of this plan.
2. Building marshals and alternates are assigned as follows:

Building Marshal Alternate Marshal

Historic Campus—Vice President for Finance and Administration
Continuing Education Center—Vice President for Continuing Education
Mooresville Center—Director of the Mooresville Center
Cherry Street Center—Director of Safety, Energy Management and Security
South Statesville Skills Center—Director of South Statesville Skills Center
Cosmetology Center—Cosmetology Program Director

3. Building marshals and/or alternates are responsible for:
    a. implementing this plan in an actual emergency
    b. supervising practice drills
    c. posting and updating evacuation escape routes for all rooms in their building
    d. coordinating and scheduling, with the maintenance engineer, periodic safety inspections to detect and correct potential fire and safety hazards in their building
    e. insuring that personnel who work in their building are familiar with this plan.

C. Fire

1. Any person who detects a fire in a building should immediately activate the nearest fire alarm and then notify the MCC Security (5444) or senior college official by the quickest means possible. Whenever an alarm is activated, it will sound throughout the building. The MCC Security Department will notify the Statesville Fire Department (704-878-3425) whenever a panel alarm is activated, or whenever they receive word from any other source of a fire in a building.
2. When an alarm sounds in a building, Building Marshals, supervisors, and instructors shall urge immediate and orderly exit by all persons by means of the published escape routes

(Appendices C1-C6) and assemble in the designated areas (Appendix C7). The building marshal will ensure that the building is evacuated. Faculty and staff members will remain with the students in the designated assembly area until a decision is made by the administrator in charge either to reenter the building or to disperse. When reentering a building, the maintenance engineer and/or his staff will turn off and reset the fire alarm.

3. Once the Statesville Fire Department arrives, the administrator in charge and the building marshal will confer with the Fire Chief to determine what assistance, if any, he may require from MCC personnel.

D. Bomb Threats

1. Any employee of Mitchell Community College who receives a bomb threat against the College should attempt to get as much as possible of the information contained on the checklist in Appendix D. This form should be available at all workstations that have a telephone. Once the threat call is completed, the person receiving the call should notify the administrator in charge immediately.
2. The administrator in charge will cause the fire alarms to be sounded in all buildings.
3. The MCC Security (before 5:00 P.M.), The Director of Safety, Energy Management, Security or the MCC Security Officer on duty (during the evening) will immediately contact the **Statesville Fire Department** (704-878-3425) and the **Statesville Police Department** (704-878-3406). If the threat is not specifically directed to the Main Campus, the off-campus centers: Continuing Education Center, Statesville, and Mooresville Center, Mooresville also will be notified.
4. When an alarm sounds, all persons will immediately evacuate the building using the published escape routes (Appendices 1-6) and assemble in the designated areas (Appendix 7). The building marshals will ensure that the building is evacuated.
5. The administrator in charge will request assistance from and confer with the Fire Chief and/or police representatives to determine what actions 110 are to be taken. A building search will be conducted only at the direction of the fire/police chiefs and under their supervision.
6. Faculty and staff members will remain with the students in the assembly area until a decision by a senior administrator, after consultation with local police, fire department, and/or bomb search personnel, will decide when to permit reentry to the building(s) or to disperse.

E. Violent Acts

1. Any person who observes or detects a violent or threatening situation where physical harm may occur should: a. immediately dial 911 and request assistance, and b. notify the MCC Security (704-880-0923 or Campus radio) or, if after 5:00 p.m., the MCC Security (704-880-0327 or Campus Radio).
2. MCC Security will attempt, during normal hours, to immediately notify one of the senior administrators (VP's and Deans) with priority of notification being the Vice President for Finance and Administration.

F. Other Emergencies

1. Any person who detects a life-threatening situation on the campus will immediately dial 911 and request emergency assistance.

2. During normal hours (8 a.m. - 5 p.m.), the person should then notify the MCC Security (704-880-0923 or Campus Radio) who will in turn notify a senior administrator.
3. After normal hours (5 p.m. - 10 p.m.), all persons will notify the MCC Security (704-880-0327 or Campus Radio).

G. Practice Drills

1. A day and an evening fire drill will be conducted in all buildings at least once every six (12) months.
2. A practice bomb threat will be conducted in all buildings once a year.
3. Drills may be announced or unannounced.

<u>See Appendix C for Evacuation Routes:</u>
C-1 Evacuation Routes, Main Building
C-2 Evacuation Routes, LRC Building
C-3 Evacuation Routes, Science Building
C-4 Evacuation Routes, Vocational Building
C-5 Evacuation Routes, Student Center Building
C-6 Evacuation Routes, Continuing Education Center
C-7 Evacuation Routes, Cherry Street Center
C-8 Evacuation Routes, Cosmetology Center
C-9 Evacuation Routes, Mooresville Center

8.14.00 CAMPUS SECURITY

Mitchell Community College employs three full-time and a varying number of part-time security personnel. During registration and other events MCC may hire off-duty officers from the Iredell Sheriff Department.

Additionally, all employees are responsible for being aware of their surroundings and taking steps as needed for the security of the campus. These steps might include any of the following: intervening with a request for the situation to be terminated; calling a senior administrator or professional; reporting the incident to the College Receptionist with request for assistance; or call the Statesville Police Department (704-878-3406).
Students at Mitchell Community College will be informed of this policy at orientation, and it will be included in the **College Catalog**.

A. Campus Security Act

Congress has passed a Campus Security Act which requires the College to record certain crimes. The Mitchell Community College Campus Safety Team will be responsible for developing a campus security policy; reviewing the policy regularly; and updating the policy as needed.

For purposes of satisfying the requirements of the Campus Security Act at Mitchell Community College, all instructional areas will be considered to be those locations at which credit courses are taught: MCC Main Campus, Continuing Education Center, Cosmetology Center, Cheery Street Center and the Mooresville Center. An annual report will be prepared by the Director of Safety, Energy Management and Security in September, and forwarded to the Vice President for Finance and Administration.

The report includes occurrences of crimes listed below.

B. Definitions of Crimes Which Must Be Reported

1. **Murder**: The willful (non-negligent) killing of one human being by another.
2. **Rape**: The carnal knowledge of a person forcibly and/or against that person's will, or not forcibly or against that person's will where the victim is incapable of giving consent because of his temporary or permanent mental or physical incapacity; or an attempt to commit rape by force or threat of force.
3. **Robbery**: The taking, or attempting to take anything of value under confrontational circumstances from the control, custody, or care of another person(s) by force or threat of force or violence and/or by putting the victim in fear of immediate harm.
4. **Aggravated Assault**: An unlawful attack by one (1) person upon another person wherein the offender uses a weapon or displays it in a threatening manner, or the victim suffers obvious severe or aggravated bodily injury involving apparent broken bones, loss of teeth, possible internal injury, severe laceration, or loss of consciousness. **Note**: an unsuccessful attempt to commit murder would be classified as an aggravated assault.
5. **Burglary** (breaking or entering): The unlawful entry into a building or other structure with the intent to commit a felony or a theft.

Note:
Forced entry is not a required element of the offense so long as the entry is unlawful (constituting a trespass) - it may be accomplished via an unlocked door or window. Included are unsuccessful attempts where force is employed or where a perpetrator is frightened off while entering an unlocked door or climbing through an open window.

The College must also report the number of arrests for the following crimes that occur on campus: liquor law violations, drug abuse violations, and weapons possession. An arrest has occurred when a law enforcement officer has detained an individual with the intention of seeking charges against the person for a specific offense(s) and a record is made of the detention.

C. Definitions of Crimes for Which Arrests Must be Reported

1. **Liquor law violations**: violations of laws or ordinances prohibiting the manufacture, sale, purchase, transportation, possession or use of alcoholic beverages (with the exception of driving under the influence or drunkenness).
2. **Drug abuse violations**: violations of laws prohibiting the production, distribution, and/or use of certain controlled substances and the equipment or devices utilized in their preparation or use.
3. **Weapons possessions**: violations of laws or ordinances prohibiting the manufacture, sale, purchase, transportation, possession, concealment or use of firearms, cutting instruments, explosives, incendiary devices, or other deadly weapons.

D. Incident Report Form

An "Incident Report Form" must be filled out by anyone who observes or is connected with handling of any of these crimes:

1. Murder
2. Rape
3. Robbery
4. Aggravated Assault
5. Burglary (breaking or entering)
6. Liquor law violations
7. Drug abuse violations
8. Weapons possession

Copies of the Incident Report Form will be available in all administrative Offices, in the Faculty/Staff Lounge and Appendix E herein. An Incident Report Form should be filled out immediately following observance of one of the incidents listed and the completed form turned over to the Dean of Instructional Services for inclusion in the Annual Security Report.