Navajo Technical University

Disaster Recovery Plan

Version 1.0

Table of Contents

Section 1: General Information

I. Introduction to the Plan
II. Objectives and Overview

Section 2: Disaster Planning

I. Disaster Risks and Prevention
II. Disaster Preparation
III. Backup Procedures

Section 3: Initiation of Emergency Procedures

I. Safety Issues
II. Information Technology Disaster Notification Accountability List
III. Activating the Disaster Recovery Plan
IV. Equipment Protection and Salvage
V. Damage Assessment
VI. Emergency Procurement Procedures

Section 4: Initiation of Recovery Procedures

I. Cold site preparation
II. Platform Recovery Procedures
III. Applications Recovery Procedures
IV. Critical Applications

Section 5: Maintaining the Plan

I. Maintenance of the Plan

Section 1: General Information

I. Introduction

In order to effectively deal with disaster situations that would seriously affect academic and business processes at Navajo Technical University, NM, the Department of Information Services has developed a comprehensive disaster recovery plan for computing and telecommunications operations.

In the event of a disaster in the main technology and telecommunication hubs at Navajo Technical University, this plan shall be used to guide the recovery and business continuity processes of critical departments on campus. This information will be available on hard copy documents as well as the campus information services website and CD-ROM disks. Hard copies will also be filed with multiple administrative offices. The master document will be held personally by the Chief Information Officer, Information Technology Director, Network/System Administrator, Database Administrator, and Web Master.

II. Objectives and Overview

Navajo Technical University depends heavily on computers, software, and networks for day-to-day business and academic activities. Every department now requires hardware, software, networks and information technology personnel to complete some or all daily tasks.

This document is meant to provide a functional and evolving plan that is followed by the College's Information Services Department in the event of a disaster.

Although this document is meant to avoid catastrophic loss of data and systems, all disaster plans assume a certain amount of risk. The success of this plan is not only dependent on using this guide for recoveries but to evaluate and plan for new types of technology disasters. No disaster plan can be certain on the variables of a wide-spread disaster and how much data can be recovered.

Time is also a factor in the equation. Time in the acquisition of equipment, software and installation are always factors to consider. This plan DOES NOT guarantee zero data loss and zero down time. Significant effort will be required to:

1.) Acquire replacement equipment
2.) Restore data integrity to the point of the disaster
3.) Synchronize that data with any new data collected from the point of the disaster and beyond

Primary Objectives

1. Outline a viable course of action for restoring critical computing and network capability to the Navajo Technical University campus.

2. Describe an organizational structure for carrying out the plan.

3. Provide information on personnel that will be required to carry out the plan and the computing expertise required in the event of a recovery (both internal and external to the institution).

4. Identify equipment, software and other items necessary for recovery.

An overview of the plan is as follows:

1. Personnel necessary for recovery (skill sets, qualifications, security clearance, etc.)

2. Salvage Operations at the Disaster Site (protective and reactive measures) and temporary physical relocation site(s)

3. Recovery process accountability (staff accountable for tasks necessary)

4. Purchase of new equipment (staff accountable and vendors necessary)

5. Recovery of both the physical platform equipment/networks and operating systems software

6. Restoration of application data (user/departmental databases and files)

7. Support communication and data services around the campus

8. Return to a stable computing and network environment.

Section 2: Disaster Planning

I. Disaster Risks and Prevention
Although it is impossible to describe every possible disaster threat, this plan takes into
account both nature and human-created disasters such as:

- Fires
- Floods
- High Winds and Threatening Weather
- Earthquakes
- Computer crimes
- Terrorist activates and/or sabotage
- Aviation disasters
- Other foreseen disasters.

a. Fires
i. Fire Alarms are in place throughout the campus buildings. Alarms are also present in
the Cave where the campus server and communication head ends operate.

ii. Fire Extinguishers are in place throughout the campus buildings and the Cave. Hand held fire extinguishers are required in visible locations throughout the buildings.

iii. Halon Systems were once employed as a viable fire suppression solution but due its after effects other systems must be installed. Today's solutions include systems that do no harm to electronic equipment, storage media, server room personnel and the ozone.
iv. Recommendations:

1. Regular inspections of fire alarms and hand held extinguishers are
done by campus operations on a regular basis. Likewise, non-disruptive tests on the non-Halon system should be done on a regular basis to increase the likelihood of its success in a disaster situation. These tests are costly.

b. Floods

i. Location: The Information Service areas, which include both the main office and the server and communication head end, are located in separate buildings that are surrounded by higher ground. Flood waters have been known to penetrate the Cave
on rare occasions. Campus storm sewers and outside modifications have been made to alleviate the threat but to little avail. There are no major water or sewage pipes near the cave to cause any issues.

ii. Recommendations:

1. Inspections should be made on a regular basis to the garage door of the machine room to detect water seepage and excessive air conditioning condensation.

2. Water detectors should be installed in the machine room and tested on a regular basis.

3. Information Service staff should be trained in responding to victims of electrical shock.

4. Information Service should be relocated to a space on campus above ground or that is better sealed to outside water and mold contamination as well as internal water carrying pipes and drains.

c. High Winds and Threatening Weather

i. Recommendations:

1. All occupants of all campus builds should be trained on the strongest points in the building and the technology staff should monitor a weather radio to assess the imposing threat.

2. Information Services should have large tarpaulins or plastic sheeting available in the machine room area ready to cover sensitive electronic equipment in case the building is damaged.

d. Earthquakes

i. Recommendations:

1. Preventative measures are similar to a threatening weather as building construction determines whether the facility will survive or not.

2. Information Services should have large tarpolines or plastic sheeting available in the machine room area ready to cover sensitive electronic equipment in case the building is damaged.

e. Computer Crimes

i. Preventative measures in place

1. All systems are protected by security products installed to protect against unauthorized entry. Levels of security include: passwords, system level logging, access lists (user/machine level) as well as firewall-based security measures. Virus control software as well. Control the proliferation of viruses among systems. Note: While we do take great care in putting security measures in place, no system connected to a network can ever be certified to be 100% secure.

ii. Continuation of operations

All security and virus systems and measures should be assessed on a regular basis to ensure they are up-to-date with the latest hacks, viruses and bugs. Continued updates and upgrades should be done on firewall equipment and software to ensure the best protection against data intrusion.

f. Terrorist action and sabotage

i. Preventative measures

1. Good physical security through security personnel checks, employee background checks and locks for authorized personnel areas are being researched and tested.

II. Disaster Preparation

During a disaster situation, there are many dependencies that are present. Many departments will not be able to resume normal operations without certain resources such as information services and the business office.

As each individual office develops a plan to resume operations, each should include ways that it can resume operations manually while Information Services recovers. Examples
of this are payroll, security, and physical plant.

a. Recovery Facility

In the event that the Information Technology Department offices are destroyed in a disaster, recovery of that facility may take an extended amount of time. In this event, an alternate location for operations must be found.

There are a number of options but with each comes additional costs.

Options include:

i. Hot Site -The most expensive of the options, a hot site would give the College, in fact, two operations centers with two physically separate machine rooms and space for staff. This hot site would be outfitted to double our current computing facilities and network operations. This solution would include additional equipment, software and personnel.

ii. Disaster Recovery Company-Local companies and colleges in New Mexico offer services for alternate/backup data center operations. This would entail running two systems in tandem, one production and one hot production backup. This is also very costly for not only duplicate equipment but data circuits to an alternate location center. While there is serious concern about the costs for a full alternate location, a disaster recovery company would be helpful in housing and storage of remote backups off-site.

iii. Disaster Partnerships-There are a number of local colleges, universities, high schools, and government entities that may be interested in partnering with Navajo Technical University in disaster recovery locations and backup systems. These entities may include: University of New Mexico, Dine' College, Indian Health Service, NTUA, Crownpoint High School and UNM-Gallup. Operations such as computer hardware/software, payroll, classroom space, accounts payable and account receivable are examples of how partnerships could be used. This option seems to be the most feasible of the options given the costs involved.

iv. Cold Site-A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired. This site would include equipment, software and network equipment adequate to install and restore for operations. This site differs from a "hot site" in that it is simply a space with equipment necessary to resume operations.

v. Replacement Equipment-In the event of a disaster, it is, of course, extremely important to have replacement equipment if the operations center/ machine is destroyed or damaged. This equipment would come from vendors such as IBM, Cisco, Harris, APC, and Motorola as would include items for both system and network operations. A list of needed equipment and vendor contacts are included within this planning document.

vi. Backups and Recovery

1. Automated tape backup
2. Remote Dual Copy

3. Off-site tape backup storage
4. Storage Area Network Back
5. Department Network Attached storages

vii. Backup Procedures

1. Internal processes available upon request to the System and Networks Administrator

Section 3: Initiation of Emergency Procedures

I. Safety Issues-refer to physical plant's hazardous materials documentation

II. Information Services Disaster Accountabilities

a. Director of Information Technology

i. Call to report and direct all staff members in the assessment and recovery process of information systems and services to the campus and report to the emergency management team.

ii. Coordinate and assess information technology needs with department heads across the campus.

iii. Coordinate vendor contacts, services and purchases necessary to resume information services to the campus in case of outage or damage.

iv. Assess the financial needs of the recovery operation and report to emergency management team.

v. Coordinate utility and facility needs with Director of Operations and necessary outside contractors.

vi. Coordinate with Marketing Communications on web site updates either on-site or off-site via co-location system services.

vii. Document all financial and support activities for archives and insurance purchases and reports. STAFF RESOURCES ACCOUNTABLE: All Information Technology Department staff

b. Director of Information Technology

i. Direct and assist programming staff and contractors in carrying out the duties of assessment and recovery of College administrative systems and services and report to Director.

ii. Coordinate needs and resources with other administrative staff to facilitate recovery of necessary administrative systems.

iii. Make recommendations to the CTO on courses of action needed in their area.

iv. All equipment, software or services purchases must be approved by the Director and/or CTO before being carried out.

v. Keep record of all contractors and expenses incurred within their area and report them to the CTO and/or President for approval. STAFF RESOURCES ACCOUNTABLE: director of information services, administrative IT personnel.

c. Systems, Networks and Database Administrators (Senior Staff Members)

i. Direct and assist I.T. staff and contractors in the assessment and recovery of network systems and servers.

ii. Located and acquire equipment and services necessary to resume network operations.

iii. Communicate and coordinate circuit and equipment needs and staff resources to the Senior Staff group

iv. Make recommendations to the Director on courses of action needed in their area.

v. All equipment, software or services purchases must be approved by the Director before being carried out.

vi. Keep record of all contractors and expenses incurred within their area and report them to the Director for approval. STAFF RESOURCES ACCOUNTABLE: Hardware repair technician, operations assistant, Integrated Systems Programmer/Analyst, Web Content Coordinator, I.T. Senior Staff

d. Information Technology Director

i. Assist in the direction of internal staff support activities.

ii. Setup and operate the Help Desk and support services to the campus

iii. Communicate needs and resources to the Senior Staff group.

iv. Make recommendations to the Director on courses of action needed in their area.

v. All equipment, software or services purchases must be approved by the IT Director before being carried out.

vi. Keep record of all contractors and expenses incurred within their area and report
them to the Director for approval.

vii. ID card operations for students, faculty and staff as well as external contractors and aid workers should be done through this response area. STAFF RESOURCES ACCOUNTABLE: Audio/Video Coordinator, User Support Group, Hardware repair technician, Web Content Coordinator, I.T. Senior Staff

e. Coordinator of Telecommunication Services (Senior Staff Member)

i. Direct and assist Telecommunications staff and contractors in the assessment and recovery of telephony equipment, systems, and networks.

ii. Locate and acquire equipment and services necessary to resume telecommunications operations.

iii. Communicate and coordinate circuit and equipment needs and staff resources to the Senior Staff group

iv. Make recommendations to the IT Director on courses of action needed in their area.

v. All equipment, software or services purchases must be approved by the IT Director before being carried out.

vi. Keep record of all contractors and expenses incurred within their area and report them to the IT Director for approval. Print and distribute all contact numbers (cellular and line-based) to all staff, faculty and students immediately after acquisition and distribution of telecommunications resources. STAFF RESOURCES ACCOUNTABLE: Telecommunications staff, Hardware repair technician, Senior I.T. staff

f. Senior staff contact numbers

Director of Information Technology x14193 – home (505) 786-4193

Telecommunications Coordinator
X14195

Dean of Instruction for Instructional Technology
X14113 – home (505) 862-0160

g. Other staff contacts Programmer/Analyst-Moodle
x14168

Telecommunications Assistant
X14195

Operations
X14307

Data Assessment Director/Marketing
X14111

Coordinator of Student Computing/ Manager of the Bookstore
X14180

Telecommunications Technician
X14195

Computer Support Specialist
X14319

Media Center
X14129

Desktop Computer Support Specialist / Virus Specialist
X14319

Dean of Student Service/ Administrative Computing
X14104 – home

Systems & Networks Administrator
X14194 – home (505) 786-7549

Integrated Systems Programmer/Analyst
X14194

Computer Support Specialist
X14319

Administrative Secretary
X14157

Programmer/Analyst-Moodle
X14168

System Analyst
X14152

Computer Repair Technician
X14319

III. Disaster Recovery Teams-Director of Information Technology supervises all teams listed. Staff listed as lead will carry out tasks and manage process and progress. Staff members were selected for these teams on the basis of their primary expertise and area of specialization within Information Technology.

a. Damage Assessment and Recovery Management Team-Assessment of physical and data damage and oversees priorities in hardware/software/network systems

- CTO
- Director of Information Technology (functional lead)
- Systems and Networks Administrator
- Dean of Student Services/Administrative Computing
- Dean of Instruction/ Instructional Technology
- Coordinator of Telecommunications

b. IT Office Coordination Team-communications and procurement

i. Administrative Assistant (functional lead)

ii. Operations Assistant

c. Equipment Acquisition Team – servers and computer hardware

i. Systems and Networks Administrator (functional lead)

ii. Coordinator of Telecommunications

iii. Desktop Support Specialist

iv. Computer Repair Technician

v. Administrative Assistant

d. Recovery Management Team – Administrative Enterprise Resource Planning (ERP) systems

i. Assistant Director for Administrative Computing (functional lead)

ii. Systems and Networks Administrator (

iii. Systems Analyst / HelpDesk Coordinator

iv. Programmer/Analyst

v. Programmer/Analyst

vi. System Analyst

vi. Consultants and recovery team

e. Network Recovery Team

i. Director of Information Technology (functional lead)

ii. Systems and Networks Administrator

iii. Integrated Technologies Programmer / Analyst

iv. Coordinator of Student Computing

v. Outsourced network installation (UNM ITS)

f. Web-site recovery

i. Integrated Technologies Programmer / Analyst (functional co-lead)

ii. Web Content and Design Coordinator (functional co-lead)

iii. PHP Web Hosting as service provider /

g. Computer and Software Installation and Support Team

i. Dean of Instruction/ Instructional Technology (functional lead)

ii. Desktop Support Specialist

iii. Desktop Support Specialist

iv. Desktop Support Specialist

v. Coordinator of Student Computing

vi. Systems Analyst

vii HelpDesk Coordinator

viii. Audio/Video Manager

h. Telecommunications Recovery Team

i. Coordinator of Telecommunications (functional lead)

ii. Systems and Networks Administrator

iii. Telecommunications Assistant

iv. Telecommunications Technician

v. Outsourced switch installation and configuration team (i.e. InterTel)

vi. Outsourced circuit providers-/Sprint/Qwest/Frontier

i. Radio Communications Recovery Team

i. Integrated Technologies Programmer / Analyst (lead-radio communications)

ii. Operations Assistant/ Finance (lead-equipment procurement)

iii. Coordinator of Telecommunications (lead-PBX communications)

IV. Disaster Recovery Priorities – Priorities are set by assessing the risk and liability associated with each process and system in Information Technology.

a. Communication of information to Internet viewers – Support Marketing Communications in updates and other information to the web.

b. Telecommunications – telephones and external circuits (telephony and data)

c. Administrative ERP – payroll, student records, schedules, accounts receivable, accounts payable, financial aid, etc.

d. Core network systems-network equipment/lines, routing, domain name systems, web systems, electronic mail, backup systems

e. Secondary functional systems-course management, calendaring, event management, etc.

f. Environmental systems – air and heating for machine room – resourced from Physical Plant

g. Helpdesk operations and hardware/software support, installation

V. Activating the Disaster Recovery Plan Activation of a Disaster Recovery Plan is a function of the President of the College and the Administrative Council. This group will assess the situation and will notify all administrative officers of a disaster situation.
The following is a list of items that must be addressed with the process of activation:

a. Appointment of a Recovery Supervisor-In the event of a disaster, the most appropriate supervisor for Information Technology is the Director of Information Technology. If the Director of Information Technology is not able to fulfill this duty, the appointment should be made by the Dean of Instruction or by the President. This person must have data center management experience and must have signature authority for the expenditures necessary during the recovery process. Please refer to Section 3, II for accountabilities for the Director and staff.

b. Determine Personnel Status – One of the Recovery Supervisor's important early duties is to determine the status of personnel working at the time of the disaster. Safety personnel on site after the disaster will affect any rescues or first aid necessary to people caught in the disaster. However, the Recovery Manager should produce a list of the able-bodied people who will be available to aid the recovery process. The Recovery Supervisor should also quickly appoint the any team leaders needed if teams
leads listed are not available. The Human Resources, Campus Ministry or other designates will work with families and employees, ministering to their needs and obtaining counseling services as necessary.

Taking care of our students and employees is a very important task and should receive the highest priority immediately following the disaster. While we will have a huge technical task of restoring computer and network operations ahead of us, we can't lose sight of the human interests at stake.

c. Establish an IT recovery operations center and salvage equipment/backup media-This location should be found first and all salvageable equipment and software should be retrieved to this location. If the Science and Technology building site is unusable, another site should be identified with the proper environment (dry, HVAC, electrical, etc.) necessary for computing operations.

d. Activating the Disaster Recovery Plan

i. The Recovery Supervisor should locate the lock box/safe that the disaster recovery document is contained.

ii. The Recovery Supervisor should appoint the remaining members of the recovery teams and reallocate as necessary.

iii. The Recovery Supervisor should meet with the teams all together and address the following areas:

1. The Recovery Supervisor reviews the Disaster Recovery Plan with the teams and special personal or College issues should be discussed and finalized.

2. Each team should review the status of their areas of accountability.

3. After this, a location for the recovery should be found and approved by the Recovery Supervisor and the Vice President and Dean of Faculty.

4. Make clear who is accountable for each area in the plan and who is to begin the work.
5. Team members are to immediately start the process of procurement, support and recovery.

6. The Recovery Supervisor is charged with directing all of the teams and team leads are charged with setting up regular meetings with the teams to assess progress and problems.

7. Distribution of radio/cellular communications devices should be targeted and updated on ETA as soon as possible.

VI. Equipment Protection and Salvage
This section outlines basic information on procedures to be used following a disaster to protect and salvage resources in a damaged area:

a. Protection and inventory

i. Gather all magnetic tape cartridges into central areas and cover with tarpolines or plastic sheeting to avoid water damage.

ii. Cover all computer equipment to avoid water damage.

iii. Alert security to post security guards at the site to prevent theft or vandalism

iv. Return any salvaged equipment and media to the recovery center

v. Take an inventory of all equipment and media recovered and report to Recovery Supervisor

b. Recovery of salvaged equipment and media

i. Attempts at this process will be done and reports on these pieces will be reported for the damage assessment process.

VII. Damage Assessment

a. This process is preliminary to assess the damage to hardware and software as well as the operations center. The primary goal is to assess effects to priority systems in order for hardware and software media to be ordered as soon as possible. Team members should be realistic in the time that is estimated to repair and restore critical systems. The teams should collaborate on the dependencies that will be present with multiple projects in progress.

b. Reporting should be carried out in the following format:

i. Hardware equipment that is salvageable and parts that are needed to recover it

ii. Assess the damage to software and take necessary steps to recover it

iii. Assess the equipment and software that is missing or unsalvageable

iv. Report on needs and systems recoverable and complete documentation on equipment, configuration and software needed to recover systems that are NOT recoverable from salvaged pieces

Section 4: Inventory overview and Vendor Contacts

I. Hardware assets & value assessment (as of winter, 2004)

a. Number of College owned computers installed: 663 (2003 in-cycle numbers only)

b. Total number of students computers supported: 600 (2003 ResNet numbers)

c. Total number of computers supported campus-wide: 1,000 (2003 numbers)

d. Number of student accessible computers: 250

e. Percentage of students who bring computers to campus: 30% (2003 ResNet numbers)

f. Number of College owned network laser printers installed: 40

g. Total replacement cost of computers/printers installed: $100,000 (2003 market value)

h. Campus ratio of Windows computers vs. Mac computers: 97% to 3%

i. Total replacement cost of network equipment installed: $500,000.00 (in renewal process now)

j. Total replacement cost of central computer server equipment: $300,000.00

k. Replacement cost of telecommunications switch and equipment: $1,000,000.00

l. Replacement cost of audio/video equipment: $100,000.00 (2007market value basis)

II. Software inventory assets & value (dated winter, 2004)
a. Campus standard operating systems: Microsoft Windows 2000/XP, Apple OS 9.2/10.x , Linux

b. General use: Microsoft Office, MOODLE, Microsoft SQL server 2005, Adobe Creative suite 3

c. Statistical use: SPSS

d. Campus standard server operating systems: LInux, Microsoft Windows Server

e. Yearly cost for all software licenses campus-wide: $500,000 (2007 market value basis)

III. Vendor Contacts

In development