

Disaster Recovery Plan for Restoring Critical Information Systems and Services

Northern Essex Community College

Contents

Overview	2
Distributing the Plan	2
Assessing Risk.....	3
Mitigating Risk.....	3
Maintaining the Plan.....	3
Setting Priorities.....	4
Declaring a Disaster	4
Notifying the Disaster Recovery Team.....	4
Activating the Alternate Site.....	5
Determining Hardware and Software Requirements	5
Hardware Requirements.....	6
Software Requirements	6
Implementing the Recovery Procedures	6
Data Recovery	6
Restore Procedures.....	7
Evaluating the Major Areas.....	8
Designing a Reconstruction Plan.....	8
A. Disaster Recovery Checklists.....	10

Revision Date: October 30, 2009

Overview

The scope of this disaster recovery plan for Northern Essex Community College addresses scenarios where the information systems and related technological infrastructure are physically damaged and/or require relocation due to; fire, flood, electrical, sabotage by personnel, malicious attack, or some other harmful event.

For the purposes of this plan, information systems refer to software applications and network services under the centralized management of the College's Information Technology Network Operations (IT NOC) Center and Management Information System (MIS) departments. Technological infrastructure refers to the cabling, servers, networking equipment, and management systems used to maintain the availability of information systems. This recovery plan is exclusively designed to restore these College assets in the event of a disaster.

Business continuity goes further, including everything beyond the recovery and restoration of information technology to keep specific College operations functioning following a disaster. This may include telephones, alternate sites for employees, procedures for keeping in touch with employees, students, and suppliers in the event that normal operations are disrupted for extended periods of time. These additional measures, while prudent, are beyond the scope of this particular plan.

Distributing the Plan

This Disaster Recovery Plan must be distributed to the following people:

- Chief Information Officer (CIO)
- Director of Information Client Services (ICS)
- Director of Information Technology Network Operations Center (IT NOC)
- Members of the Disaster Recovery Team (copies stored at residence)
- Main Computer Room (primary site is A Building)
- Buildings and Grounds Dept. in Haverhill
- Alternate sites (Lawrence and North Andover Campuses)
- Offsite with the back-up tapes

The Chief Information Officer shall decide if further distribution is needed. The residence copies provide offsite planning capabilities in the event a disaster occurs during non-working hours or that the computer room at NECC is totally destroyed.

The maintenance of the Northern Essex Community College Disaster Recovery Plan is the responsibility of the Chief Information Officer and appropriate staff. Part of this responsibility encompasses the distribution of current versions of the disaster recovery plan to all key personnel.

Assessing Risk

There is not enough information available at this time to fully quantify the expected financial loss or other operational impacts (based upon duration, time of year, and other factors) resulting from a specific disaster or crisis. Therefore, a formal and comprehensive risk assessment is not possible as part of this plan. The risks identified within this contingency plan are to be considered a subset of risks within the context of an overall business continuity plan.

Mitigating Risk

The institution provides adequate facilities to house, maintain, and operate information systems and sustain acceptable levels of system security and reliability. Even though all root causes of potential malicious attacks and environmental risks can never be completely eliminated, many with the highest probability of occurring can be prevented. Major events, such as a malicious attack or a natural disaster are very unlikely to occur and are beyond the capacity of Northern Essex Community College to prevent in most instances. Other factors are within the control of College, at least in terms of reducing the risk of certain events. The facilities within the ITNOC Computer Room incorporate reasonable provisions to mitigate risks with a higher probability of occurring.

- Electrical provisions
- Backup power
- Cooling
- Water detection
- Physical structure
- Space utilization
- Physical access

The college has also made significant investments in networking infrastructure, redundancy, backup systems, and management utilities in order to mitigate the damaging effects of unavoidable system failures. Most of the critical components of the computing network have built-in redundancy and fault tolerance. Information technologies employed to mitigate the impact of malicious physical attacks or the damaging effects of environmental events will continue to be upgraded, replaced and introduced based on strategic priorities, changes in technology and available funding.

Maintaining the Plan

This plan must be re-evaluated on an annual basis in order for it to remain current and operational, as technology and electronic equipment change. The plan must be adapted to the most recent acquisitions of technology. This requires that a list of installed hardware and software be maintained.

Information should be solicited annually from managers and senior staff concerning improvements to the existing systems that have occurred during that time frame and should be incorporated into the Disaster Recovery Plan.

Setting Priorities

It is impossible to foresee all possible scenarios that may require a disaster recovery response. Therefore, this plan represents procedures that may need to be adapted depending on circumstances. However, safety is always the foremost concern (regardless of the circumstances) followed closely by legal requirements and then the operational necessities of the college. Priorities may differ based on the time of year (for example, financial aid), day of the week (for example, time and attendance entry), or even time of day (for example, when classes are in session).

This plan is intended to provide a reliable and flexible response, with responsibility shared among teams of people. The essential components of this plan include activating the plan, notifying the appropriate people, securing an alternative site location, recovering the technological infrastructure, and then restoring the information systems and services.

Declaring a Disaster

A disaster or emergency is defined as an event that could endanger personnel or resources or both as opposed to an interruption of services that is limited in scope or duration. The Chief Information Officer (CIO) or the Chief Financial Officer (CFO) has the responsibility of declaring a disaster. In their absence the President of the College or any of the leadership team management can declare a disaster.

Use Table 1 to determine the authorized personnel to contact about the disaster. All of these people are to be informed of the declared emergency, and that the recovery plan has been activated, by the CFO.

Table 1. Personnel Authorized to Declare a Disaster

Name	Ext.	NECC Cell	Home	E-mail
David Hartleb, President	3855	978 360-3855		dhartleb@necc.mass.edu
Mary Ellen Ashley, Executive VP	3627	978 360-7339		meashley@necc.mass.edu
Sue Wolf, CFO	3921	978 360-7860		swolf@necc.mass.edu
Jeffrey Bickford, CIO	3745	978 4769720		jbickford@necc.mass.edu

A more general communications plan informing faculty, staff, students, and suppliers will be formulated by the appropriate member(s) of the college's senior management team depending on the scope of the operational impact.

Notifying the Disaster Recovery Team

Technical response team members (shown in Table 2) are to be contacted as needed by the College's Chief Information Officer, or the Chief Financial Officer, and will work under that officer's direct authority to recover the technological infrastructure and restore information systems.

IMPORTANT NOTE: If an event takes place with staff onsite at the Network Operations Center (NOC), it is critical that all employees and personnel be accounted for. Campus Police have established protocols and evacuation plans for each building in case of emergency.

In the case of an emergency or disaster affecting more than the IT NOC Computer Room, Campus Police are to be in charge of the total emergency response operation, in conjunction with the Haverhill Police Dept., the Haverhill Fire Dept., and Emergency Medical Services.

Table 2. Core Technical Response Team Members

Dave McAskill (Director)	978 360-4460 (NECC cell)
Mark Cloutier (Telephone System & Voice Mail Issues)	978 360-4459 (NECC cell)
Bonnie Moore (Network Manager)	978 360-4461 (NECC cell)
Phil Wysocki (Network Administrator)	978 360-5790 (NECC cell)
Scott Proctor (Windows Exchange Manager)	978 360-7286 (NECC Cell)
Cyndi Sawyer (Backups)	978 360-8712 (NECC cell)
Mike Kolotila (Systems Analyst)	978-420-2789 (NECC cell)
Kathy Riviezzo (Database Administrator)	978-408-6964 (NECC cell)

Local Emergency Numbers

Ambulance 911

Campus Police X3689 or 1-978-556-3689

Third Party Service Providers and Technology Suppliers (Emergency Contact)

See the Vendor Phone Numbers List stored separately [].

Activating the Alternate Site

Northern Essex Community College has an alternative data center location at 45 Franklin Street in Lawrence Massachusetts and also at 1600 Osgood Street in North Andover Massachusetts. The NECC Disaster Recovery Team must contact the director of the alternate site and inform that person of the situation at NECC.

This location has an active connection to the Internet for Northern Essex Community’s use along with sufficient facilities to host and operate the College’s administrative and student information systems, e-mail system and website in the event of an emergency.

Determining Hardware and Software Requirements

Several components are critical to the effective operation of the NECC information systems. These include the following, with the first several being considered the most critical:

- Networking
- Banner/Oracle
- E-mail server
- Middle tier infrastructure (metadata repository)
- Web services (college web site, Self Service)
- Document imaging

- SQL server
- Blackboard (academic content delivery system)
- Blogs and faculty web sites
- eLumen (tracking students at risk)
- ARGOS (a reporting tool to be implemented by 2010)

The following two sections describe the hardware and software requirements for restoring core functionality of the college's administrative and student information systems, e-mail system, and web site in the event of a disaster or catastrophic failure of systems.

Hardware Requirements

Hardware requirements define the physical server hardware and platforms required to support critical NECC systems based on existing production hardware and manufacturer's recommendations. Since hardware is updated or replaced over time, details of these requirements and a Network Infrastructure Diagram are maintained in a separate document called Hardware Software Maintenance.xls.

Software Requirements

Software requirements define the operating systems, network utilities, and software applications required to support critical NECC systems based on the existing production configuration and the manufacturer's recommendations. Since software is updated or replaced over time, details of these requirements are maintained in a separate document called Hardware Software Maintenance.xls.

Implementing the Recovery Procedures

The following sections describe the methodologies for restoring core functionality of the College's administrative and student information systems, e-mail system, and web site in the event of a disaster or catastrophic failure of systems. This includes the materials and steps necessary to build the systems from the ground up and restore each system to an operational state.

A Disaster Recovery Checklist and a Reconstruction Plan Checklist are provided in Appendix A.

Data Recovery

All critical data for NECC systems is part of a regular tape backup cycle designed to insure data integrity and availability in the event it needs to be restored. Data is written to tape via a weekly full and daily differential backup schedule. The specifics of the NECC backup and retention schedule are defined below. As an additional safeguard, tapes are also brought offsite on a weekly basis to insure adequate data safety.

Backup Files and Schedule

Since backup files and schedules are subject to change depending on business requirements, this information is stored in a separate document called Backup Schedule.xls.

Tape Retention

Table 3 identifies the type and frequency of backup tapes.

Table 3. Tape Retention Schedule

Backup Type	Retention Period
Nightly (Differential)	8 Weeks
Weekly (Full)	8 Weeks
Off-site Storage (Full)	2 Months (Haverhill full database backup tapes are manually brought to North Andover Campus each week). End of month backups are stored indefinitely with backups being brought offsite monthly. Haverhill tapes are stored in North Andover, North Andover tapes in Lawrence, and Lawrence tapes in Haverhill.

Backup Hardware Specifications

Since backup hardware is periodically updated or replaced over time, the specifications are stored in a separate document called Backup Schedule.xls.

Restore Procedures

Use the following steps to restore systems.

Prerequisites:

1. A declaration of emergency was made by an authorized personnel member, as defined under the section on Declaring a Disaster.
2. Notification was sent to the required technical team members by the CIO to assess the situation, define systems in need of restoration, and to coordinate the next steps.

Procedure:

1. Hardware and equipment are to be secured for specified systems, as defined under the section on Determining Hardware and Software Requirements.
2. Hardware is brought to the alternate as determined by the Disaster Recovery Team.
3. Hardware is installed in pre-existing racks and configured as needed.
4. Load the operating system, load required applications, and restore data.
5. Software configuration is verified, as defined in the preceding section on Data Recovery.
6. IP address is changed to reflect the NECC networking configuration. Designations for systems are available in a separate document called ITNOCinfo.xls.
7. DNS entries are updated in external DNS servers located at the alternate site to reflect new IP Address. DNS server information is available in a separate document called ITNOCinfo.xls.
8. Connectivity to new systems is tested and verified.

9. Pending successful testing and verification of rebuilt systems, notification is made from technical team members to the CIO.
10. The CIO notifies appropriate campus parties the system has been restored, as defined under the Notification section of this document.

Evaluating the Major Areas

After establishing a working secondary site, and making sure that all aspects of Northern Essex Community College's processing needs are functioning, the Disaster Response Team should focus on the restoration of Northern Essex Community College's primary site. The following areas of concentration should be examined:

Physical Plant

Discussions should be commenced with the Building Management to ascertain the structural integrity of the primary site and to develop charts to track the progress of scheduled repairs. During this process, senior staff should be regularly apprised of the progress.

Public Utilities

Each utility should be contacted and asked for the anticipated date for restoration of service. This would include water, telephone, electric, plus any code inspections that might be required.

Data Processing Equipment

The MIS staff in concert with the Disaster Response Team should survey the equipment and determine if it is operational. If it is found that repairs or replacement are required, the procurement process should be initiated and tracked for timely execution.

Cabling

The College should contact the necessary contractors to have them certify that the communications wiring in the primary site is ready to resume full operational status.

Designing a Reconstruction Plan

The steps necessary to restore the primary site will vary widely depending on the type of disaster that is experienced. The following factors should be considered when developing a Reconstruction Plan:

Project Schedule

Development of a chart to map the progress of the project. Define who will be the source of direction in returning to the primary site.

Site Restoration

Define who will be responsible for the interface with the appropriate authorities if the primary site has been totally destroyed. Determine what responsibilities are to be assumed by Northern Essex Community College.

Equipment

Determine who will be responsible for deciding whether or not to replace the existing equipment with duplicate products, or whether this is a good time to evaluate options.

Backups

Determine if off site backups are going to interface adequately with the recent equipment decisions and employ media that will facilitate any changes in architecture.

Users

Have the personnel of Northern Essex Community College been notified of the changes necessary to migrate back to the primary site? Have transportation and equipment issues been adequately addressed?

Reconstruction Checklist

A Reconstruction Checklist is available in Appendix A.

A. Disaster Recovery Checklists

The Leader of the NECC Disaster Response Team is responsible for maintaining the master checklist, and providing updated copies to the team members as needed. These lists include the Disaster Recovery Checklist and the Reconstruction Plan Checklist.

In any crisis situation having a written summary or steps to be executed ensures that a systematic approach to the problem is adopted. These lists should guarantee that all facets of the situation receive the necessary remedial action.

The Disaster Response Team is responsible for the coordination of all Recovery Plan details and the physical recovery of equipment, supplies, software, salvage operations, acquisition plans, and the restoration of the complete operation of NECC. The Disaster Response Team Leader must maintain a schedule that prioritizes systems and applications that are critical to NECC operations.

Disaster Recovery Checklist

Recovery Activities
Initiate recovery plans to save data and move processing to the alternate site if necessary.
The Disaster Recovery Team will assist Northern Essex Community College with notification of insurance, fire, police officials, and public relations as well as any additional resources deemed necessary
As soon as possible the Disaster Recovery Team Leader will notify the CIO of the need for direction and assistance in initiating operations at the alternative site.
As soon as possible the Disaster Recovery Team must contact Senior Staff whose sections are dependent on computer operations. The following types of assistance will be requested:
Collection of source documents Communication of the current situation to Northern Essex Community College Personnel Re-directing the flow of data to the alternate site.
Instruct users to adopt previously defined manual (non-electronic) operations.
Plan for the transportation of MIS staff and materials to the backup site.
Notify users of the status of the DRP through frequent status updates.
At the time that operations are commenced at the alternate site, the Disaster Recovery Team Leader will designate selected personnel to maintain salvage operations and secure the physical plant at the damaged site. As allowed by public safety authorities.
Make arrangements to provide regular shuttle service between the primary and alternate sites to move necessary materials.
Develop a system to re-route necessary mail service to the alternate site
The status of the files should be made available to the Senior Staff member responsible for that application, so that they can decide on the restoration policy and the utilization of specific backup media.
Develop a system to assist users in reconciling reports.
Record an entry in the Operator Log as each application including system software is restored.
Develop and maintain a schedule for recovery of system applications.

Reconstruction Plan Checklist

Reconstruction Plan
List in detail damage to the physical unit and all equipment, including supplies. Prepare an evaluation of the damage.
Issue current status reports to senior staff and end users.
Develop and maintain a system of charts to delineate the progress of the project.
Consult with Hardware vendors relative to the possible repair or new acquisitions.
Discuss software replacement with vendors. Be sure to include supporting documentation.
Track and orchestrate re-building and repair functions at the primary site.
Establish anticipated delivery and installation schedules.
Arrange for re-supplying the office to include: desks, chairs, paper supplies, writing instruments, and reference materials.
Develop a plan for testing new equipment.
Develop a planned timetable for testing of recovered applications including system software. Each item should be logged as it is processed
Are repairs and re-construction projects completed at the primary site?
Is all hardware installed and operational?
Has all software been restored to the same condition that existed before the disaster?
Has all software been tested and is ready for resuming operations?
Do you have a final backup from the alternate site?
Is the backup ready for restoration to the system at the primary site?
Have all the supporting documents been returned to the primary site?
Have you notified College personnel that processing will return to the primary site?