

Berea College

Disaster Recovery, Business Continuity, and Network Redundancy Plan

Prepared by:
Office of Information Systems and Services

January 27, 2005

Revised May 23, 2006

Revised May 30, 2007

Revised July 29, 2008

Revised August 25, 2009



Approved by Administrative Committee **Date**

Approved by Board of Trustees **Date**



Table of Contents

1. Executive Summary	2
2. Overview	3
a. Technology Infrastructure Disaster Planning	
b. Personal Computer Data and Software	
c. Information/Communications Infrastructure	
3. Contingencies (Events Covered Under This Policy)	6
4. Prevention Strategies	7
a. Network Path Redundancy	
b. Equipment Component Redundancy	
c. Power Protection	
d. Environmental Control Systems	
e. Fire Protection	
f. Physical Access Control	
g. Physical Separation of Data Backup Media From Servers	
h. Network Security and Virus Threat Monitoring and Response (Response & Communication Procedures)	
5. Readiness Procedures (Activities and Safeguards in Place to Ensure Response Readiness)	9
6. Recovery Team and Task Groups (Duties and Responsibilities)	10
7. Recovery Process (Methods for System and Infrastructure Recovery)	11
8. Business Continuity During Recovery (Overview of Critical Processes and Basic Approach to Continuity)	14

Appendices

1. Appendix A - Administrative/Academic Applications	15
2. Appendix B – Contact Information for the Incident Recovery Team	16
3. Appendix C – Member Responsibilities for Recovery Team	17
4. Appendix D - Data Backup and Media Retention Policy.	18
5. Appendix E – Network and Server Equipment List and Suppliers	19
6. Appendix F – Checklists of Off Site Storage Recovery Resources	20
7. Appendix G – Possible Additional Prevention Strategies <i>(Includes additional Network Redundancy possibilities).</i>	21
8. Appendix H - Alternative Work Flow When Primary Systems are Down During Recovery Effort	22

Executive Summary

Berea College operates a complex technical infrastructure to support our academic programs, student services, and administrative functions. Operations across campus are highly dependent on this infrastructure, and therefore plans must be in place to prevent disruptions, address disaster contingencies and ensure business continuity in the event that system disruptions occur. This policy identifies potential threats or contingencies that could have catastrophic consequences for college operations. The policy also describes our prevention strategies to reduce risk, outlines readiness procedures which would promote a quick response to a disaster incident, and describes the team structures and methods we would follow during a recovery scenario.

This policy addresses various risks including fire, severe weather, sabotage, power failure, virus attacks, and operator error among others. The most common events include server or network equipment failure and power interruptions. Fire and intrusion are also considered high risks that require preventative measures. Physical protection and security, equipment component redundancy, fire extinguishing systems and climate control systems are among the many preventative measures in place. This policy includes specific schedules, methodology, and assignments for staff responsible for carrying out routine preventative measures involving data backups, storage/rotation of backup media, climate control, security and more.

Strategies for reducing risk and preventing disaster will be implemented whenever it is possible and affordable to do so. On an annual basis prior to our EDP audit, our policy will be updated to reflect prevention strategies in place (see page 7) and prevention strategies under consideration (see appendix G). This will create a current "state of affairs" for an annual external review. As part of our annual external audit, audit firm personnel will assess this information against current industry standards & benchmarks and provide recommendations to us that will shape our priorities for the upcoming year.

While each disaster event is unique, our response to each event follows a common pattern which includes communication activities, incident assessment, establishment of recovery teams and task groups, recovery methods, and priorities for specific restoration activities. The appendices are designed to demonstrate that work flow and to guide the College through a recovery event. These appendices identify priority systems, recovery team responsibilities and membership, offsite storage schedules and locations, equipment suppliers, offsite recovery resources and more. Appendix H outlines alternative work flow and methods to support business continuity during a system outage or recovery from a disaster event.

This policy also directs the College to maintain at a safe offsite location, certain resources that may be needed to support recovery from a disaster event. These resources include documentation or backup copies of data, software configurations, application software, technical manuals, and procedures associated with critical systems. A copy of this policy will be included among these resources.

Each year, Berea College intends to review and update this policy and pursue strategies that reduce the risk of system outages that could disrupt core business and instructional activities. The annual external audit will allow us to have an independent review of this effort on a routine basis to ensure that all reasonable actions are being taken to protect our technology assets and promote the reliability and availability of these key systems to our constituencies.

Overview

A. Technology Infrastructure Disaster Planning

Berea College operates a highly complex technical infrastructure to support our academic programs, student services, and administrative functions. Operations across campus are highly dependent on this infrastructure and therefore, plans for disaster recovery, business continuity, and network redundancy are essential and must be well articulated and accepted across campus. This policy identifies potential threats or contingencies that could have catastrophic consequences for college operations, describes prevention strategies that reduce risk, outlines readiness procedures so that we are able to quickly respond to a catastrophic event, and describes the team structures and methods we would follow during a recovery event.

Berea College is committed to an ongoing effort to enhance the dependability of our technology infrastructure and reduce the risk of component failure. We have established processes for data backup and the storage of key resources and information off site so we can rebuild systems in the event of a catastrophic event. In addition, we have identified critical business processes that will need to continue during an extended system outage and documented the basic approach that would be taken to continue these processes during the restoration process.

Our preparedness strategies focus being able to recover from catastrophic damage to one or more of our major network and server hub locations - the Computer Center, Lincoln Hall, and the Bruce Building Annex. The goal of the strategies is to enable recovery of all critical infrastructure services within three weeks of a disaster event. Scenarios involving less catastrophic loss would employ a subset of plans and recovery resources and would probably require less time.

B. Personal Computer Data and Software

Security and availability of restorable backups for campus microcomputers are the responsibility of individual users. Individuals should backup key data on their personal computers as outlined in college policy. Training is available from IS&S and tools are available for personal computer data backup.

IS&S offers access to a Data Backup Server. Faculty and staff can maintain a current backup of their personal computer data files and documents on this server. For Windows computers a script package is available which allows one-click initiation of backup of My Documents, Desktop, and other commonly modified resources from the PC to the server. A commercial backup program is available for Macintosh users. Virtually all personal computers at Berea College are equipped with some form of high-capacity backup device, usually a zip drive or CD writer. The presence of this type of high capacity media allows clients to create an offline copy of their backup server data area quickly and efficiently and they can store this backup in a secure location offsite.

C. Information/Communications Infrastructure

The following infrastructure is supported by IS&S and are considered critical systems/services that must be considered when planning for disaster scenarios:

1. Virtual Server & Storage Infrastructure:

- Virtual Server environment running on 3 Dell PowerEdge VMWare Infrastructure 3 hosts.
- Virtual disk storage volumes managed on 2 EMC Clariion 12 TB SAN arrays.

2. Enterprise Systems:

- SCT/BANNER 2000 version 7.x running on HP9000 server Oracle 10g database with Oracle 10g Application Services running on Dell PowerEdge Windows 2003 server.
- NOLIJ document image services running on Dell PowerEdge Windows 2003 server
- Special forms print services running on Windows 2008 virtual server hosted under our VMWare virtual infrastructure.

3. Courseware:

- Blackboard Basic Edition running on Dell PowerEdge Windows 2003 server.
- Moodle running on Windows 2003 virtual server hosted under our VMWare virtual infrastructure.
- CAN-8 Foreign Language lab and resources running on Dell PowerEdge Windows 2000 server.

4. Email/Web Mail:

- Microsoft Exchange 2007 running on 3 Dell PowerEdge Windows 2003 servers, one for Faculty/Staff mail, one for Student mail, and one for send/receive and address list hub services.
- Barracuda Anti-Spam appliance in front of mail servers for filtering spam mail

5. Network Domain Access Control & Identification Services:

- Domain Control running on 2 Dell PowerEdge Windows 2003 servers
- Domain Name Services running on 2 Dell PowerEdge Windows 2003 servers
- DHCP Services running on 2 Dell PowerEdge Windows 2003 servers
- Cisco NAC device for registration of client devices allowed on the network
- WSUS server for security updates pushed to client devices

6. Print Services:

- Windows network print queues running on Dell PowerEdge Windows 2003 servers
- Equitrac Express pay for print & photocopy software running on Windows 2008 virtual server hosted under our VMWare virtual infrastructure.

7. Software License Management:

- Sassafras K2 and FLEXIm license management software running on Dell PowerEdge Windows 2003 server

8. Web Services:

- College web site running on 3 Dell PowerEdge Windows 2003 servers for the main web site, student and community group web sites, and SQL databases.

- Enterprise Portal web application running on Dell PowerEdge RedHat Linux server with databases on a Dell PowerEdge Windows 2003 SQL server.

9. Departmental FileMaker Database Systems:

- Groups of databases running on 2 Dell Windows 2003 virtual servers hosted under our VMWare virtual infrastructure.

10. Departmental File Sharing:

- Running on 5 Dell PowerEdge Windows 2003 servers for Academic and Administrative departments and 1 Dell PowerEdge Windows 2003 server for IS&S technician resources.

11. Network Infrastructure:

- 2 Cisco backbone routers located in the Computer Center and Bruce Building Annex data centers connected via fiber optic cable to Cisco and/or Nortel layer 3 switches in each campus building.
- NetMon monitoring device for analysis of network traffic problems.

12. Internet Connection:

- Cisco ASA firewall located in Bruce Building Annex Communications Room
- Windstream-owned edge router for connection to KPEN Internet service
- BlueCoat web filtering device
- PacketShaper web traffic management device

13. Phone System:

- Nortel Meridian 81C PBX supplemented by 2 Personal Computers running MATSCH billing software, and AVOTUS phone services management software
- Cisco Call Manager 6 server for IP phones.

14. Voice Mail:

- Nortel Call Pilot proprietary system running on PC hardware
- Cisco Call Manager 6 server for IP phone user voicemail.

15. Library System:

- Ex Libris Voyager software running on Sun Microsystems Sun Fire V240 server configured and maintained by Ex Libris.

16. Building Security & Access:

- Stanley Security Systems running on 2 central personal computers to control locks for the Computer Center, Bruce Building Annex, EcoVillage common area and all residence halls. Standalone programmable electronic locks in Frost building and Science building are not affected by central resources.

Contingencies

Events Covered Under this Policy

The following events may invoke this policy as they pose risk to our data and/or telecommunications infrastructure:

- Flooding
- Fire
- Weather (tornado, wind damage, or other natural phenomenon)
- Sabotage, interdiction, or network security breach
- Climate control failure involving temperature and humidity
- Power interruptions, either brief or extended
- Equipment failure
- Accidental destruction or corruption of data

Depending on the severity of damage to the physical space, power supply, or environment controls, different strategies for recovery could include:

- Recovery of damaged resources at the original site.
- Relocation of operations to an alternate site on or off campus, possibly with a reduced level of service.
- Transition of services to the original site from the temporary alternate site, possibly with a reduced level of service for a period of time. (See [appendix A](#) for Essential Administrative & Academic Applications)

A disaster will be declared, and the incident recovery plan will be invoked when an event has disabled, or is expected to disable, key computing and communications facilities to the degree that normal operations will be significantly impacted.

Every disaster situation is different and therefore the first step of response is to immediately assess the particular situation and promptly develop a recommended course of action using this document as a guide.

Once issues involving the protection of personnel have been addressed, priority will be given to shutting down and protecting key systems, securing data, transferring equipment to safe locations, and implementing the recovery plan.

Prevention Strategies

Strategies for reducing risk and preventing disaster will be implemented whenever it is possible and affordable to do so. Berea College has implemented a number of such prevention strategies. The following sections outline prevention/risk reduction strategies in place. Appendix G provides a list of prevention strategies under consideration by Berea College IS&S. The most common sources of system failure involve power interruptions and equipment failure – especially power supply and disk drives. Fire and intrusion are also considered high risks worth an investment in prevention.

A. Network Path Redundancy

Links between the three primary network hub locations of the main campus (Computer Center, Lincoln Hall, and Bruce Building Annex) are such that if one path is broken, the equipment can be reconfigured to follow an alternate path. For instance, if the direct link between the Computer Center and Lincoln Hall hubs is broken, the network closet cabling can be reconfigured to pass the signals through Draper building using spare fiber cables along the routes between the Computer Center and Draper and between Draper and Lincoln Hall.

B. Equipment Component Redundancy

Most servers are configured with redundant power supplies and RAID disk systems. A RAID (Redundant Array of Independent Disks) system writes each data sector to two locations on separate disks. Control logic then allows the system to continue processing data even if one of the hard drives fails and allows for easy replacement of a failing drive within the array.

C. Data Center Redundancy [NEW]

The former telecommunications equipment area in the Bruce Building Annex and the Network & Server Room in the Computer Center are located across campus from each other. Both spaces are outfitted with a full set of data center environmental protections. Virtual server and storage host resources are located in both data centers. This will allow critical virtual resources to be consolidated to one of the two locations if the other is damaged. It also allows data backup server resources to be located in a protected space while also being physically separate from the servers being backed up.

D. Power Protection [IMPROVED]

Critical servers, network equipment, telephone equipment and server room climate control equipment in the Computer Center and Bruce Building Annex data centers are protected by battery backup systems and generators such that a power outage of less than 48 hours should not affect operations.

Network backbone facilities in Lincoln Hall and network building interface switches are equipped with individual Uninterruptible Power Supply (UPS) systems, providing 30 to 45 minutes of battery power in the event of power failure or significant degradation of incoming power. Non-critical servers located in the Computer Center are protected with a 20 KVA APC UPS unit rated to provide several hours of battery power. The APC unit sends e-mail to network services personnel to notify them of power outages and restorations. Upon a loss of central site power that lasts more than five hours, the IS&S Network Services Team is expected to use the available UPS backup time to insure that manual shutdown procedures are initiated, and to monitor automated shutdown procedures to verify that they are progressing normally. Shutdown procedures should be initiated after five hours of power loss. IS&S staff must communicate with the Facilities Management department to insure they are aware of the outage, as they have primary responsibility to interface with the power company and to determine best estimate of repair times.

Power conditioning and UPS services do not extend to desktop computers and printers. In the event of widespread power outage, critical processes that depend on desktop computers and printers may have to be moved to an alternate location that is not affected by the outage. Desktop computers and printers are connected to surge protection power strips to prevent damage due to occasional power problems. Those individuals using laptops will be able to perform a normal shutdown of their computer in the event of a power failure by using their built-in battery.

E. Environmental Control Systems [IMPROVED]

Our two data centers are cooled by air conditioning systems separate from the building HVAC. These devices are protected from power outage by generators.

F. Fire Protection

Each of our data centers are protected by an automatic HALON based fire extinguishing system. The system is periodically serviced and tested. The service contracts are maintained by Facilities Management. Disaster recovery resource materials are stored in a fireproof data safe located in the Bruce Building Annex area.

G. Physical Access Control [IMPROVED]

The primary network backbone switches, servers and phone systems are located in our Computer Center and Bruce Building Annex data centers. Entrances to the Computer Center, Bruce Building Annex and to the data center rooms are secured by BEST Access Systems electronic locks activated by ID card swipe readers. The Computer Center entrance is automatically locked between the hours of 5:00 p.m. and 7:55 a.m. weekdays and at all times on weekends. The data center rooms and the Bruce Building Annex entrance are locked at all times. All Information Systems and Services staff have access to the building entrances at any time by using their staff ID card. Access to the data center rooms is granted only to those staff and students whose job duties require entry.

Building network closets are accessible only by Mechanical Room keys issued to personnel whose job duties require entry.

H. Physical Separation of Data Backup Media From Servers

In order to reduce the risk that original and backup data would be destroyed in the same disaster event, data backup media are stored in locations physically removed from the servers on which the data resides. Data backup servers are located in different campus buildings from the servers on which the live data resides.

I. Network Access Control [NEW]

Cisco Network Access Control systems require that any piece of equipment connected to the network be identified in a registry which documents who is responsible for the equipment and checks to verify that virus protection and current Windows security patches are present. Such controls reduce the risk that virus infected equipment could connect to our network or that malicious activity could occur without accountability or detection.

J. Server Virtualization [NEW]

Using virtual server hosting software, we have set up redundant hosting environments. Rather than purchasing a small server for each application, a few large servers are set up as application server hosts and extra capacity is installed to allow for redundancy. Each application server is deployed as a guest on a virtual server host and can be backed up as a full configuration image. If a hardware failure occurs on one host, virtual servers can be quickly restored from images and deployed on another host.

K. Network Security and Virus Threat Monitoring and Response

Network-related problems due to viruses, a security breach, attempts to circumvent network security, or denial of service attacks could escalate into a disaster if not addressed at an early stage. IS&S has initiated monitoring and response procedures to reduce the risk of such a disaster. IS&S technicians check informational web sites frequently to become aware of new threats. Network traffic through the central router is monitored several times each day, and any unusual activity is investigated. Upon detection of virus activity or intrusion attempts, the network port involved is quarantined until the source is demonstrated to have been removed. Network users are encouraged to report security concerns or suspicious activity to the IS&S Network Services Team.

When incidents occur, communication regarding diagnosis, prevention and cleanup is provided to network users and the Help Desk. Individual workstations and/or laptops found to be a source of the problem are blocked and/or given restricted bandwidth. This process protects other network users

and maintains the stability of the network. However, if a major virus outbreak occurs, IS&S can shut down network service to specific buildings or sections of buildings using VLANs. This process allows us to isolate a major virus outbreak quickly. Network service would then be restored to buildings (and sections of building) as viruses are removed. In the event of a major virus outbreak, priority will be given to restoring service to mission critical activities as noted in Appendix A.

Readiness Procedures

Activities and Safeguards in Place to Ensure Response Readiness

The activities below must be performed on an ongoing basis to insure Information Systems & Services is prepared to address incidents that invoke this procedure.

- All IS&S personnel are informed of their responsibilities in the event of an incident (see appendix C). Responsible Individual: IS&S Senior Technical/Administrative Analyst
- Routine data backup processes (including the periodic rotation of backup media to off-site locations) are strictly followed. The offsite backup schedule for Information Systems & Services is provided in appendix D. Departmental guidelines require that the most current backup tapes are removed from the tape drives and stored in an offsite location on a daily basis. Responsible Individual: IS&S Network Services Coordinator
- Incident recovery resources are periodically updated – including this recovery plan document, operations procedures, technical documentation, software installation media, and system configuration information – and stored in off-site locations. A list of recovery resources is provided in appendix F. Responsible Individual: IS&S Network Services Coordinator
- Updated version of the Disaster Recovery/Business Continuity Plan is available and accessible to all campus personnel. Responsible Individual: IS&S Senior Technical/Administrative Analyst
- Emergency lighting and power systems supporting our technology infrastructure are periodically tested to ensure proper functioning. Responsible Individual: IS&S Network Services Coordinator
- Fire and smoke detection systems are tested annually. Responsible Individual: Associate Director of Facilities Management
- Uninterruptible Power Systems and generators are checked for proper functioning annually. Responsible Individual: Associate Director of Facilities Management for large central systems and IS&S Network Services Coordinator for distributed UPS devices.
- Operations procedure manuals are kept current and stored off-site. Responsible Individual: IS&S Network Services Coordinator
- Environmental standards are monitored in equipment areas daily for server room and phone switch room. Responsible Individual: IS&S Network Services Coordinator
- Berea College faculty and staff are made aware of the concept of Disaster Recovery and Business Continuity, our procedures, and how an incident could affect normal operations. This is performed annually. Responsible Individual: IS&S Senior Technical/Administrative Analyst
- This Disaster Recovery/Business Continuity plan will be reviewed annually prior to our external audit review. Documentation of system configurations will be updated, and contents of offsite storage will be verified. Responsible Individual: IS&S Senior Technical/Administrative Analyst

Recovery Team and Task Groups

Duties and Responsibilities

A Recovery Team will be assembled (see *appendix C*), when a disaster is declared by the College President in collaboration with the Administrative Committee and the Chief Information Officer. Each incident recovery team member will bring together a task group with membership based upon the types of expertise required by the particular incident. Each task group will be assigned specific tasks during incident recovery by the team leader responsible for that area as directed by the Incident Recovery Coordinator. The core Recovery Team will include the following individuals:

- A. Incident Recovery Coordinator**
(Chief Information Officer and/or IS&S Senior Technical/Administrative Analyst)
- B. Voice/Data Communications Recovery Coordinator**
(IS&S Network Services Coordinator)
- C. Administrative Systems Recovery Coordinator**
(IS&S Director of Administrative Systems and Services)
- D. Client Services Recovery Coordinator**
(IS&S Computer Center Director)
- E. Academic/Instructional Systems Recovery Coordinator**
(IS&S Instructional Technology Coordinator)
- F. Two Members Representing Client Needs**
 - Financial Services
 - Student Services
- G. Team Support Coordinator**
(IS&S Administrative Assistant)

The recovery team will set up operations in one or more of the following locations as deemed appropriate:

- IS&S Trades building 3rd floor office area
- Unaffected network hub locations (Bruce Building Annex, Computer Center)

Specific responsibilities for each member of the Recovery Team are described in *appendix C*.

Recovery Process

Methods for System and Infrastructure Recovery

Process steps to guide recovery activities are noted below:

A. Initial Incident Reporting and Assembly of Recovery Team

Anyone becoming aware of a disaster incident is asked to notify Public Safety at extension 3333. Public Safety is provided with contact information for key IS&S personnel. The first IS&S staff person made aware of the situation will immediately notify the Chief Information Officer or the Senior Technical/Administrative Analyst who will determine if members of the Recovery Team need to assemble.

B. Safety and Access Evaluation

Public Safety personnel will evaluate the physical area affected and determine what safety measures should be taken and what access restrictions need to be put in place. They will also initiate rescue or medical emergency response as appropriate.

C. Initial Incident Assessment

The Recovery Team will develop an incident report that outlines the extent of damage and the equipment/supplies/personnel likely needed to orchestrate a quick recovery of vital systems.

The report will be sent to the Administrative Committee.

D. Recovery Team Task Groups Established

The Recovery Team will be established and personnel will be assigned to Task Groups. The Incident Recovery Coordinator will develop priorities after a full damage assessment has been performed. The recovery team will focus on high priority areas first, including the protection of existing assets, the restoration of basic data and voice communications capabilities, essential data processing functions as outlined in Appendix E, and later, full restoration of all client desktop applications.

E. Recovery Plan Established

After initial actions are taken to secure and protect systems and equipment from further damage, an incident recovery plan will be developed and forwarded to the Administrative Committee for approval to proceed with needed expenditures (equipment, supplies, or additional expertise) and remaining recovery efforts. It is expected that this planning and approval will occur within 24 hours after notification of the incident. The plan should consider the need for various supplies not normally considered part of a replacement equipment order. These supplies may include electrical cables, fiber patch panels and cables, copper connectors, etc. Also, a quick inventory will be performed of essential equipment and supplies on hand to determine what materials can be salvaged and what supplies and material need to be ordered. The President will authorize, if appropriate, emergency procurement of replacement equipment bypassing normal purchasing procedures. The VP of Business and Administration will arrange for insurance carriers to be notified of the incident.

The central computing facility uses primarily Dell, Nortel, Cisco and Hewlett Packard equipment which is readily available from either the manufacturer or used equipment suppliers and can be acquired within a few days to a week. Assuming that assessment can be completed and approval obtained within one or two days after a disaster event, it is expected that equipment could be brought in within one to two weeks and critical services restored within two to three weeks depending on the number of services impacted.

F. Interim Communications Methods Established

A temporary web site may need to be set up at an alternate location. Means of communicating among team members and with the campus community will need to be set up. Responsibilities will be assigned for communicating with media, local government, student parents, etc. and for keeping web site information up to date.

G. Emergency Business Procedures Invoked

Offices will be notified of the service interruption, and critical processes will be switched to manual or other alternative procedures. More detail about critical processes and alternative procedures is found in the next section of this document which outlines approaches to business continuity during the recovery effort.

H. Equipment and Services Procured

A review of any usable equipment in inventory or in use for non-essential purposes will be made to determine if any lost services can be restored without purchase of new equipment.

Emergency orders will be placed for any equipment, supplies, or media needed. Vendor service representatives will be contacted to expedite shipment of components that require immediate delivery. Other suppliers will be contacted to see if faster delivery or better prices can be obtained.

Records of all expenses and copies of source documents for replacement equipment or for services will be kept and supplied to the Business and Administration office for submission with insurance claims.

Vendor technical support services (such as Banner, HP support etc...) will be contacted when assistance is needed and their involvement in recovery efforts will be coordinated by the Recovery Team.

A listing of network and server equipment, vendors, contact names, and telephone numbers is provided in Appendix E.

I. Restoration Site Determined

If the central site cannot be used to restore service, an alternate location will be activated. In that event, the Administrative Committee will be informed that an alternative site will be necessary to continue operation. Possible alternative sites may include:

- Bruce Building Annex (if Computer Center only is damaged)
- Computer Center (if Bruce Building Annex only is damaged)
- IS&S Trades Building 3rd floor offices
- Lincoln Hall network hub closet

If an alternative location is needed, the Recovery Team will coordinate the transfer of equipment and support personnel into the alternate location.

J. Partial Restoration of Services

1. As soon as basic equipment is (re)assembled, recovery task groups will load operating systems and operational software, restore data from backup resources, and commence testing and certification procedures.
2. Initial recovery work will focus on establishing security control and basic network and voice communications services for the interim operations environment.

3. Recovery task groups will restore network connectivity where possible to areas that have been made inaccessible by the event. Emergency orders will be placed for any materials needed to accomplish necessary splicing, testing and certification of network and communications systems.
4. If appropriate, temporary work spaces will be set up for continuance of critical services until such time as communications infrastructure can be restored throughout the campus. A recovery task group will be responsible for moving personal computers and other equipment to the temporary work spaces.
5. Priorities for the restoration of department operations will be determined and the appropriate recovery task groups will load any special software packages in order of most critical need.
6. Data backup media and other recovery resources will be returned to offsite protected storage as soon as possible.
7. Critical operations will be restored, resuming production and backup procedures as facility capacity is restored.
8. Schedule will be followed to ensure that all critical support services are restored as prioritized (See *Appendix A*).
9. College administration, staff, faculty and students will be informed of status, progress, and problems as appropriate.

K. Return to Normal Operations

1. If an alternate site has been utilized, the Recovery Team will coordinate activities for restoration of the original site and for moving equipment back to the original site with minimal disruption of operations.
2. If temporary work spaces have been utilized, equipment will be moved back to original locations when communications is restored.
3. Offices will need to process backlogs of transactions and otherwise transition from alternative procedures back to normal processing.
4. Recovery Team will develop long range plans for full restoration of any services that remain impaired.

L. Follow-up Activities

1. Assist Business and Administration office with filing of insurance claims.
2. Review Disaster Recovery Plans and make revisions based on recovery experience.

Business Continuity During Recovery

Overview of Critical Processes and Basic Approaches to Continuity

A critical process is a business process that must continue during the time that the technology infrastructure and primary systems are unavailable during the recovery effort. The following approaches will be used as an alternative until primary systems can be restored.

Source Document Staging: Source documents will be accepted and stored for later processing on the recovered systems.

Paper Filing: A filing system will be devised to store paper source documents for retrieval and for later processing on the recovered systems.

Manual Process: Manual processes for filling out handwritten forms and routing them for approval and/or action will be used to process transactions. Most manual processes will also involve later processing of catch-up transactions on the recovered systems.

PC Process: A temporary log or document generation process will be set up on a personal computer. The process may need to work without access to network resources. Most PC processes will also involve later processing of catch-up transactions on the recovered systems.

Alternate Process: An alternate process is available that could be used. For instance, if web based ordering is the usual procedure, and the Internet is down, a phone ordering procedure may be available.

Alternate Location: The process can be moved to an alternate location, such as an area of campus unaffected by communications failure or an off campus facility with Internet access.

See [Appendix A](#) for a prioritized list of major applications that may require recovery and [Appendix H](#) for more detail on specific processes and alternative work flow options.

Appendix A - Administrative/Academic Applications

Administrative and academic applications which are dependent on our technology infrastructure and their relative importance to Berea College operations are listed in the chart below.

Note that "Important" and "Convenient" areas may be essential functions which are considered less dependent on the technology infrastructure. These areas could remain unavailable until essential applications are brought online.

Business Function	Application Module or Resource	Priority
Accounts Payable	BANNER Finance	Essential
Student Accounts	BANNER Student	Essential
Admissions	BANNER Student	Essential
Building Security & Access	Stanley Security Systems	Important
Courses/Curriculum	Blackboard	Important
Degree Audit	BANNER Student	Convenient
E-Mail	Microsoft Exchange	Important
Electronic Document Storage	Nolij	Important
File Sharing	Windows file servers	Important
Financial Aid	BANNER Financial Aid	Essential
Fund Raising	BANNER Advancement	Important
General Ledger & Budget	BANNER Finance	Important
Gift Processing	BANNER Advancement	Important
Help Desk	FileMaker database, phones	Important
Housing	BANNER Student	Convenient
Internet	Alltel (KPEN) circuit, Cisco router	Essential
Library Circulation	Voyager	Important
Language Lab	CAN-8, file sharing	Important
Network Management	Windows DC, DNS, DHCP, Cisco Router & Switches	Essential
Payroll	BANNER Human Resources	Essential
Printing	Windows print servers	Essential
Purchasing	BANNER Finance	Essential
Registration	BANNER Student	Essential
Software License Mgt.	Keyserver and FLEXIm	Essential
Student Academic Records	BANNER Student	Essential
Student Crafts Order Mgt.	COMPASS	Important
Telecommunications	Nortel PBX, Cisco Call Manager, Bell South PRI circuits, Sprint T1 line, Windstream lines	Essential
Voice Mail	Nortel CallPilot	Important
Web Portal my.berea.edu	Luminis	Essential
Web Site www.berea.edu	Microsoft IIS	Important*

* Availability of the www.berea.edu web address is an essential component of communication about a disaster incident but recovery of the normal site content is not considered critical.

Appendix B – Contact Information for the Incident Recovery Team

Team	Name	Office Phone	Cell Phone	Home Phone
Incident Recovery Coordinator	John Lympany and Bill Ramsay	3990 3342	625-2680 582-8166	none 986-6052
Voice/Data Communications Recovery Coordinator	Mike Tucker	3413	582-6261	unlisted
Administrative Systems Recovery Coordinator	Albert Conley	3353	582-1360	985-1910
Client Services Recovery Coordinator	Kevin Blankenship and Judy Gergen	3538 3307	859-473-2313 248-2009	none 200-0465
Academic/Instructional Systems Recovery Coordinator	Anthony Basham	3630	358-8573	none
Two Members Representing Client Needs	Finance – Jeff Amburgey Students – SGA Student President or designee	3088	582-8000	623-9978
Recovery Team Support Coordinator	Kay Himes	3802	248-2853	986-4806

Appendix C – Member Responsibilities for Recovery Team

- 1. Incident Recovery Coordinator**
 - a. Determines the extent and seriousness of the incident.
 - b. Assembles disaster recovery team.
 - c. Notifies the President, Provost, V.P. for Business & Administration, and V.P. for Finance of the situation and provides updates on status of the recovery effort.
 - d. Arranges for management of communication with campus community and the public.
 - e. Establishes recovery priorities and supervises recovery efforts.

- 2. Voice/Data Communications Recovery Coordinator**
 - a. Evaluate infrastructure damage (servers, network components, telecommunications equipment)
 - b. Recommend recovery steps
 - c. Work closely with CIO on laying out recovery plan and supervising recovery operation
 - d. Coordinate network/telecommunications equipment repair/replacement
 - e. Supervise restoration of system software from backup media
 - f. Keep the Incident Recovery Coordinator and other team members informed of the status of recovery procedures being implemented

- 3. Administrative Systems Recovery Coordinator**
 - a. Establish priorities for recovering enterprise system modules and bringing user departments back on line.
 - b. Include Banner resources and technical support services in recovery efforts
 - c. Coordinate with vendors on the delivery of a replacement server if necessary
 - d. Facilitate recovery activities with individual departments.

- 4. Client Systems Recovery Coordinator**
 - a. Arrange for any needed repair or replacement of personal computers and printers.
 - b. Work with other Incident Recovery Team members as an interface to the campus community to facilitate recovery efforts and communicate progress.

- 5. Academic/Instructional Systems Recovery Coordinator**
 - a. Establish priorities for restoring access to courseware systems and other instructional software
 - b. Work with Network Services as needed to restore courseware applications
 - c. Communicate with faculty on restoration process and progress

- 6. Two Members Representing Client Needs (Finance/Student Services)**
 - a. Facilitate communication between recovery team and key users to help shape priorities in restoring vital systems
 - b. Coordinate manual activities as an interim measure until systems are restored

- 7. Recovery Team Support Coordinator**
 - a. Process paperwork to order new equipment
 - b. Expedite shipment of key components by working directly with the vendor
 - c. Check for alternative sources of equipment that may help to facilitate shipment or contain costs of recovery
 - d. Follow up on needs of Recovery Task Groups for supplies, food & drink, etc.

Appendix D – Data Backup and Media Retention Policy

Purpose of policy: Establish reasonable data recovery capabilities and provide guidance to technicians and operators to inform implementation and performance of data backup processes.

1. Banner ERP and other institutional databases.
 - 1.1. Data recovery target is at most one day of lost transactions and access to data up to two months old.
 - 1.2. All data will be backed up at the end of each weekday.
 - 1.3. Backup will be to removable media which is placed in protected offsite storage by noon of the following work day.
 - 1.4. Supplemental backup to offsite disk storage is encouraged.
2. Shared network files and databases.
 - 2.1. Data recovery target is at most one day of lost transactions.
 - 2.2. All data will be backed up weekly and all changed data will be backed up at the end of each weekday.
 - 2.3. Where performance constraints or other factors prohibit the weekly/daily backup cycle, a less frequent cycle may be implemented with CIO approval.
 - 2.4. Online backup media will be located in a different data center from the server being backed up. Offline backup media will be placed in protected offsite storage by noon of the following work day.
3. Server software and configurations.
 - 3.1. Documentation of the software configuration installed on each server will be maintained.
 - 3.2. Where possible, a restorable image of server software configuration will be made after each software update.
4. Personal Computer files and databases.
 - 4.1. Data backup and recovery is the responsibility of the personal computer user.
 - 4.2. A backup script or software package and server space for one generation of data backup will be made available to personal computer users.
5. Personal Computer software and configurations.
 - 5.1. Personal computer users are responsible for installation of optional standard or specialized software on their computers.
 - 5.2. Forms for use in documentation of personal computer specialized software configuration and installation instructions will be made available to personal computer users.

6. Summary of backup operational processes and responsibilities

Server	Media	Full	Incremental	Off Site	Location	Generations
Library	DLT-4 Tape	Daily	none	Daily	Bruce Building Annex data safe	10
BANNER	LTO-2 Tape	Daily	none	Daily	Bruce Building Annex data safe	10
Windows	LTO-4 Tape, Disk Arrays	Weekly	Daily	Immediate	See note 1	3
myBerea portal	Server disk	Monthly	none	none	Portaltest2 server see note 2	1
Phone Systems	DDS125 Tape	See note 2	none	See note 3	Bruce Building Annex data safe	2

Note 1: Windows servers are backed using a set of three backup servers running Symantec Backup Exec. Each backup server is located in the opposite data center space from the servers it backs up. Each server stores data to a direct attached disk or LTO-4 tape storage array. Three generations of backup are kept – Monthly full, Weekly full, Daily incremental. A few servers for which management by Backup Exec is considered unnecessary are backed up to shared disk space on a backup server using the NT Backup utility.

Note 2: The myBerea portal is on a Linux server, but its volatile data is located on an SQL database server whose backup is handled by the Windows server processes. Configuration data, user profiles and software objects are backed up according to software vendor procedures to disk storage on another Linux server.

Note 3: Phone Systems data is backed up weekly during the high transaction activity months of August and September, and monthly during other months. Tapes are moved to offsite storage within one day after the backup is made.

Definitions:

Windows: Windows servers include all network control, e-mail and other servers that run on the Windows platform.

NAS: Network Addressable Storage; a disk storage device that attaches to a computer network and interfaces to the network security system but is not a full capability server

Daily: The operation is performed each weekday, or the night before each weekday.

Full: A complete copy of all data is sent to tape or to a NAS device.

Incremental: Any data files changed since the previous day's backup are sent to tape or to a NAS device.

Off Site: The frequency at which backup media is moved to offsite protected storage.

Generations: The number of back copies of data backup media that are kept before the media is re-used. The distance into the past that data can be recovered is a factor of the off site frequency and the number of generations kept. For instance, 10 generations of daily tapes means that the Library system can be restored to its condition as of up to two weeks prior.

Responsibilities:

- BANNER backup process setup and monitoring: Database Administrator
- BANNER tapes offsite storage: Instructional Technology Specialist
- Library backup process setup and monitoring: Library Systems Administrator
- Library tapes offsite storage: Instructional Technology Specialist
- Windows server backup process setup and monitoring: Senior Server Analyst

Appendix E – Network and Server Equipment List and Suppliers

Equipment	Supplier	Contact	Phone
BANNER Server (HP/UX)	Forsythe Technology	Tamara Schultz	847-213-7497
Windows Servers	Dell Computers	Angie Kennedy	800-274-7799 x7232789
Portal Server (Linux)	Dell Computers	Angie Kennedy	800-274-7799 x7232789
Library System (Sun)	Ex Libris	Carol Gockenbach Technical Support	847-227-2978 877-445-5693
BANNER Software	SunGard Higher Education	Neal Gold Technical Support	270-250-5500 connect.sungardhe.com
Internet Service	Alltel (KPEN)	Kent Lanham KPEN repair	859-357-6035 866-990-3282 opt 1
Internet Router/Firewall	CBTS	Kevin Klaber	513-841-5112
Network Switches	CBTS	Kevin Klaber	513-841-5112
Network & Phone Cable	D&B Electric	Dale Ballinger	859-314-2092
Local Phone Service	Bell South (KIH2)	Jennifer Robertson KIH2 repair	615-401-4012 800-563-9194
Telecomm Hardware	CBTS	Kevin Klaber	513-841-5112
For detailed list of equipment see network hardware database maintained by the Network Services Team, a copy of which is in offsite storage			

Appendix F – Checklists of Off Site Storage Recovery Resources

BANNER System

- BANNER database backup tape
- HP/UX 11.11 Operating System installation CD
- MicroFocus COBOL compiler installation CD
- Oracle 10g Database Management System installation CD
- Oracle 10gAS Application Server installation CD
- FormScape CD w/ serial number
- HP 9000 server configuration details document

Library System

- Voyager database backup tape
- Support login information sheet
- Client software installation CD
- Voyager configuration file listings
- Sun server configuration details document
- Voyager system passwords

Telecommunications Systems

- Octel voicemail data backup tape
- PBX configuration data backup tape
- Avotus TMS - data backup tape
- Avotus Order Pro installation tape
- Avotus Attendant Pro installation tape
- Avotus Intelcontrol installation tape
- CISCO stuff?

Web Site & Portal Systems

- Portal server Linux image backup DVD
- Microsoft Standard 2003 Server CD w/serial number
- Microsoft Standard SQL 2005 Server CD w/serial number
- Web server configuration backup CD
- Instructions for restoring portal, database and web server data from the backup resources.
(Server data files are backed up to a backup server tape or disk array and are not stored in the data safe.)

Network Equipment and Servers

- Microsoft Windows Server 2003 Enterprise CD w/serial number
- Microsoft Windows Server 2003 Standard CD w/serial number
- Microsoft Exchange 2007 Enterprise CD w/serial number
- Microsoft Windows Server 2008 Standard CD w/serial number
- McAfee Exchange Server Scanner CD
- McAfee Antivirus Enterprise CD
- Filemaker 7 Pro Standard CD
- Filemaker 7 Pro Advanced CD
- Filemaker 5 Server CD
- CD set of software installation resources, server and software configuration settings documentation, printer driver files, etc. copied from server storage. A table of contents file is included to describe the resources.
- Note that server data files are backed up to a backup server tape or disk array and are not stored in the data safe.

1. Network Redundancy

- **Server Redundancy/Failover:** For servers determined to require a very high assurance of availability, redundant hardware with parallel data stores and failover capability can be installed. Then if a server fails for any reason, the parallel server takes over the services.
Estimated cost: Doubles the hardware cost of each server to be set up with failover.
- **Mobile Wireless Links:** Point-to-point wireless communication equipment could be kept on hand that would allow a broken network connection to be restored quickly at a reduced service level while repairs are arranged.
Estimated cost: \$7,500 per link
- **Dual Uplink Ports:** Network routers and switches can be configured such that the links between buildings are on two ports. If one port's electronics fails, the network connection would switch over to utilize the second port.
Estimated cost: \$7,500
- **Fully Redundant Network Paths:** Upgrade our campus network such that network signals between administrative and/or academic buildings could be rerouted on an alternate path in the event of a breakdown in the usual connection. Implementation of this plan would significantly reduce the risk of down time due to network hardware failure or cable damage. Residence halls were not included in the design. The design could be partially implemented for buildings considered a higher priority. Note that we already have redundant paths between the Computer Center, Draper, Lincoln Hall and Bruce Building Annex as discussed in section 3.
Estimated cost: \$1,500,000

2. Network Security and Monitoring

- **Event Log Monitoring:** Reports could be developed which show various types of security related events that have happened on the network. Daily review of failed access attempts and certain other events could identify intrusion attempts or other network security problems.
Estimated cost: \$0 - \$5,000 depending on whether training and contract programming is needed.
- **Intrusion Detection Software:** Systems are available which automate many network security monitoring tasks. Unusual or suspicious activity can often be detected by the system which can then notify responsible personnel or initiate automated response processes.
Estimated cost: \$75,000 or more

3. Standby Equipment and/or Facilities

- **Standby Equipment Contract:** We could enter into a contract with a recovery services provider which provides access to an inventory of standby network and server equipment and operations and communications facilities for use in a disaster event. Such contracts typically also provide for annual testing of system restore capabilities at a test site.
Estimated cost: \$100,000 per year (rough estimate)
- **Alternate Central Site:** The infrastructure of an alternate campus location could be upgraded so that no network or electric power modifications would be needed in a disaster event for which operations had to be moved to an alternate site.
Estimated cost: \$10,000 - \$100,000 depending on how much readiness and reliability is planned.
- **Recovery Testing Contract:** We could enter into a contract with a recovery services provider who would provide access to server equipment similar to ours for the purpose of testing our recovery processes to verify that we have the necessary information, backup data and software installation media to recover key systems.
Estimated cost: \$1,000 - \$10,000 annually depending on the number of servers to be tested.

Appendix H – Alternative Work Flow When Primary Systems are Down During Recovery Effort

<u>Department/Function</u>	<u>Process</u>	<u>Alternate Work Flow During Recovery Effort</u>
Academic Services		
Transcripts	Process transcript request	Source document staging
Grades	Post grades	PC process
	Communicate grades to students	PC process
Graduation	Verify list of graduates	PC process
Probations	Record probation decisions	Paper filing
Convo Cards	Printing Convo Cards For Students	PC process
Enrollment Verification	Verifying that students are enrolled	Manual process
Degree Verification	Verifying that students have degrees	Manual process
Communication/Email	Communication with Faculty/Students	Manual / PC Process
Registration	Term Registration and Drop/Add	Manual process
Reports	Staff need reports on status of apps.	PC Process
Admissions		
Applications Processing	Receive/Record Application	Paper filing
Acceptance Decisions	Record acceptance decision	Paper filing
	Communicate to applicant	Manual process
Matriculation Processing	Record document receipt	Paper filing
Communication	Receiving mail in and sending out	PC Process
Test Scores	Receipt and review of student scores	PC Process
College Relations		
Gift Processing	Receive & record gift	Paper filing
	Acknowledge gift	Manual process
	Deposit gift	Manual process
Donor Contacts	Plan contacts	PC process
	Record contact events	PC process
Facilities Management		
Work Order Processing	Enter work orders	PC process
	Record order completion	PC process
Faculty Teaching		
	Post resources & assignments	PC process
	Receive assignments	PC process
	Report grades	Manual process
Finance		
Accounts Payable	Record Invoice	Paper filing
	Write Checks	Manual process
Purchasing	Create Purchase Order	Manual process
General Ledger	Create Journal Entry	Source document staging
Banking	Phone links to banks	Alternate location
Financial Aid		
Aid Packaging	Prepare aid packages	Manual process
	Send aid letters	PC process
	Getting cash to students from their aid	Manual process
	Modem links to gov't agencies	Alternate location
Reporting	Federal and State reporting	PC Process
Health Services		
	Schedule appointments	Manual process
	Record diagnosis	Source document staging

Appendix H – Alternative Work Flow When Primary Systems are Down Continued ...

<u>Department/Function</u>	<u>Process</u>	<u>Alternate Work Flow During Recovery Effort</u>
Information Systems & Services		
Help Desk	Enter service work orders	PC process
	Record inventory changes	PC process
Computer Repair	Record order completion	PC process
	Order replacement parts	Alternate process
Administration	Record purchases	PC process
	Record equipment receipt	PC process
Labor Program Office		
Labor Assignments	Record labor assignments	Paper filing
Labor Probations	Record labor probations	PC process
Library		
Circulation	Check out resource	PC process
	Check in resource	PC process
Acquisitions	Catalogue new resource	PC process
People Services		
Payroll	Set up new employees	Source document staging
	Enter payroll data	PC process
	Write checks	Manual process
	Process direct deposits	Alternate process
Hiring	Receive and record application	Paper filing
	Record hiring decision	Source document staging
Benefits	File Insurance claims via web	Alternate location
Student Course Work		
	Print documents	Alternate process
	Turn in assignments	PC process
	Access resources & assignments	PC process
	Access license controlled software	Alternate process
Student Payroll		
Payroll	Enter assignment changes	Source document staging
	Enter payroll data	PC process
	Write checks	Manual process
	Getting cash to students	Manual process
	Sending check issue file to bank.	PC Process
	Sending direct deposit file to bank.	PC Process
Student Service Center		
Student Accounts	Post student payments	PC process
Cashier	Disburse cash withdrawals	Source document staging
	Receive student payments	Manual process
	Receive deposits from other depts..	Manual Process
	Create ID card	PC process
	Grant access to residence hall	PC process