

APPROVAL, DISTRIBUTION, REVISIONS

Upon approval this **Administrative Computing Disaster Contingency Plan** will be distributed to:

1. Disaster Recovery Coordinator
2. Disaster Recovery Team Leaders
3. Director of Campus Security
4. Internal Auditor
5. Director of Risk Management
6. Off-site location where computer backup files and documentation are stored

When updated copies of this Plan are distributed, the superseded version must be completely destroyed. In the event of a Disaster everyone must be working from the same document revision. The LSSU Disaster Recovery Coordinator (named in Appendix A) will ensure all old copies are returned and destroyed as revisions are published.

Preface

This document details the Lake Superior State University Disaster Contingency Plan for Administrative Computer Processing Resources. The document provides information on the existing facilities and configurations of computer equipment and computer software used to support mainframe computer based administrative business applications.

This document also details the levels of disaster catered for and the specific recovery procedures that must be followed (and by whom) in the event of a Minor, Major or Catastrophic Disaster. This document also details the critical applications that must be recovered during a disaster to support critical University functions.

For purposes of this document the *Data Center* is defined as the room that houses the Administrative Computing mainframe computers and is located in the Administrative Computing area of the Center for Applied Sciences and Engineering Technology building.

SCT refers to the IA-Plus integrated software (or files created by) purchased from Systems and Computer Technology Corp.

DEC refers to the computer hardware and software purchased from Compaq Computer Corporation (formerly Digital Equipment Corporation)

Appendices document specific information that changes over time and contains checklists used as part of disaster recovery or preparedness.

CONTENTS

CHAPTER 1	DATA CENTER SECURITY AND SURVIVAL
CHAPTER 2	ACTIVITIES SUPPORTED BY THE ADMINISTRATIVE COMPUTING DATA CENTER
CHAPTER 3	STANDBY COMPUTER FACILITY
CHAPTER 4	APPLICATION RECOVERY PRIORITIES
CHAPTER 5	WHAT TO DO IN THE EVENT OF A DISASTER
CHAPTER 6	CRITERIA FOR ASSESSING THE SITUATION
CHAPTER 7	DISASTER RECOVERY TEAM STRUCTURES AND RESPONSIBILITIES
CHAPTER 8	DISASTER CONTINGENCY PLAN REVISIONS AND TESTING
APPENDIX A	EMERGENCY CALL LIST/DISASTER TEAM LEADERS
APPENDIX B	COMPUTER VENDOR AND GENERAL SERVICES PHONE LIST
APPENDIX C	SOFTWARE, FORMS, DOCUMENTATION, ETC STORED OFFSITE
APPENDIX D	BUSINESS RECOVERY CHECKLIST
APPENDIX E	INITIAL DISASTER RECOVERY TEAM MEETING CHECKLIST
APPENDIX F	FOLLOWUP DISASTER RECOVERY TEAM MEETING CHECKLIST
APPENDIX G	MAINFRAME COMPUTER CONFIGURATIONS
APPENDIX H	COMPUTER OPERATIONS JOB LOGS (NIGHTLY PROCESSES)

CHAPTER 1

DATA CENTER SECURITY AND SURVIVAL

The Data Center is located on the third floor of the Center for Applied Sciences and Engineering Technology building. The Center is constructed of concrete block for 3 walls and one wall of sheet rock with a reinforced concrete floor and ceiling (the ceiling is also part of the building roof). A steel raised floor sitting atop the concrete floor elevates the floor work surface to provide air conditioning ducting, electrical power cabling space, and hardware wiring space. A suspended ceiling constructed of metal grid-work and fireproof ceiling tiles conceals heat and ventilation ductwork.

An uninterruptible power supply (UPS) system provides conditioned 110-volt power to all critical computer equipment. In the event of a complete power outage, the UPS system provides battery back-up power for a period of approximately 20 minutes. This will vary depending on how quickly ancillary equipment such as printers can be powered off.

Two fireproof doors provide ingress/egress to the Data Center. One door opens directly into the Administrative Computing Office common open area and is used for normal access to the Data Center; the door has a keyed lock. The Administrative Computing Office common open area is locked from 5:00pm until 8:00am each business day and whenever the area is unoccupied during the business day. The other door has a keyed lock and functions as an exit into an adjacent hallway in event of fire but can be used as an entrance to the Data Center.

A third fireproof door provides emergency egress through an adjacent classroom; the door only opens from the Data Center side of the door.

Fire protection is provided by an ANSUL Inergen sensor activated fire suppression system. Fire sensors are located under the raised floor and at ceiling height. There are manual fire suppression activators located at each Center door. There is a conventional fire extinguisher located at each egress door. There is a conventional fire extinguisher located in the Administrative Computing Office common open area.

CHAPTER 2

ACTIVITIES SUPPORTED BY THE ADMINISTRATIVE COMPUTING DATA CENTER

2.1. Administrative Computing

2.1.1. Administrative computing is processed on a DEC AlphaServer Model 2100 computer located in the Data Center. Administrative computing is accomplished via computer software purchased from Systems & Computer Technology Corporation (SCT) and LSSU written programs that complement the SCT software.

2.1.2. SCT software modules supported are:

- Alumni Development (ADS)
- Financial Resources (FRS)
 - Financial Accounting
 - Accounts Payable
 - Purchasing
- Human Resources (HRS)
 - Payroll
- Loan Management (LMS)
- Student Information (SIS)
 - Admissions
 - Billing & Receivables
 - Financial Aid
 - Housing
 - Registration
 - Scheduling
- Z-Support (ZSS)

2.1.3. Data Backup and Protection

- 2.1.3.1. Production data files are backed-up to magnetic tape cartridge nightly, after applicable nightly update processing, and stored offsite in a fireproof file box located in Campus Security Office located in the Administration Building. Two days of backups are stored offsite.
- 2.1.3.2. During daily online update processing, each on-line transaction is written to a check-pointer data file. The check-pointer file can be used to recreate a day's online update entries in a recovery situation. The check-pointer files are backed-up as part of the production data files backup.

CHAPTER 3

STANDBY COMPUTER FACILITY

A DEC AlphaServer Model 1000 computer is setup and tested to provide standby computer processing capability in the event of a serious disaster in the Data Center. The DEC AlphaServer 1000 computer is physically located in the same Computer Operations room as the main administrative computer. At the beginning of each academic semester a Business Recovery Checklist (Appendix D) is completed to verify equipment and supplies are in their assigned place; a copy of the completed Business Recovery Checklist is sent to the Disaster Recovery Coordinator.

The SCT applications - ADS, FRS, HRS, LMS, and SIS - have been tested on the DEC AlphaServer 1000 computer to ensure software compatibility with the production SCT applications on the DEC AlphaServer 2100.

If a disaster in the Data Center made the DEC AlphaServer 2100 computer and network equipment unusable, the DEC AlphaServer 1000 computer and related stored equipment can be moved anywhere on-campus and setup to provide limited online access from a centralized location. High volume and high-speed print capacity may be reduced since only printers from other offices may be available to print reports.

If a disaster in the Data Center made the DEC AlphaServer 2100 computer unusable but left the network equipment useable, the network community would have access to the DEC AlphaServer 1000 computer from their terminals in their offices.

If forced into utilizing the standby computer, the degree of degradation with respect to computer system response time is not known, but it would certainly be significant enough to require prioritization of user access.

Chapter 4

APPLICATION RECOVERY PRIORITIES

4.1. Establishing Application Priorities

4.1.1. Critical Applications are those that must be recovered during a disaster in order to support key University functions. Each application should be identified as either:

- Essential to the University's survival (Class 1)
- To be recovered after Class 1 if processing resources are available (Class 2)
- Not available during recovery operations (Class 3)

4.1.2. The priority of recovering applications will be developed and approved by the Disaster Recovery Coordinator after consultation with appropriate users and Administrative Computing personnel. The point during the academic semester and business calendar that a disaster occurs will affect recovery priorities and schedules.

4.2. General priority for recovering applications

4.2.1. High priority (Class 1) applications are:

- Payroll
- Student grades
- Student scheduling

4.2.2. Applications to recover as more resources become available (Class 2):

- Accounting (daily)
- Student records
 - Admissions
 - Billing & Receivable
 - Financial Aid
 - Housing
 - Registration

4.2.3. Applications to recover as soon as possible (Class 3):

- Accounting (month-end/year end)
- Ad hoc report requests (FOCUS)
- Student Loan system processing
- Alumni Development system processing

CHAPTER 5

WHAT TO DO IN THE EVENT OF A DISASTER

5.1. First Steps

A disaster may create a situation in which data backups are the only surviving University records. It is natural, given the excitement and confusion of an emergency, to overlook the need to safeguard these files.

Copying data backup files and returning the originals to their off-site location must take precedence over all activity once the recovery process has begun.

In the event of a disaster within the Data Center while occupied by LSSU staff, some or all the following actions must be taken immediately depending on the nature of the event. The Director of Administrative Computing or designate or most senior Data Center employee may direct the actions.

The **FIRST** priority is to ensure the safety of all personnel.

- Determine if immediate evacuation of the Data Center is required
- Contact **SECURITY** and instruct to alert medical and safety departments
- Direct damage limiting measures to be taken if adequate time and still insure personnel safety
 - Temporarily manually override fire suppression system in order to allow assessment of the situation
 - Remove source of potential damage
 - Use fire extinguishers when appropriate
 - Initiate computer shutdown procedures for computer processing, electrical services, and air conditioning operation
 - Cover computer equipment with waterproof coverings
 - Secure and/or remove appropriate backup file media
- Use the Emergency Call List (Appendix A) to notify the Disaster Recovery Coordinator and Disaster Team Leaders

5.2. Disaster Recovery Teams

Disaster Recovery is the responsibility of:

- Disaster Recovery Coordinator
- Network Recovery Team
- Operations Recovery Team
- Systems Recovery Team

5.3. Disaster Recovery Teams Headquarters

- If the Center for Applied Sciences and Engineering Technology (CASET) Building is determined by the Disaster Recovery Coordinator to be safe, the Recovery Teams will meet in room **CAS302**
- If the CASET Building is hazardous or not usable and damage is confined to that building, the Teams will meet in the conference room in the Administration Building
- If the conference room is determined by the Disaster Recovery Coordinator not to be safe or available, the Teams will meet in the Kenneth J. Shouldice Library
- If the campus facilities are not able to be used, it is presumed the disaster is of such proportion that prompt response by the Data Center is not of paramount importance

5.4. Initial Recovery Meeting

The Disaster Recovery Coordinator, Disaster Recovery Team Leaders and Disaster Historian will meet as soon as possible after the disaster occurs. The purpose of the meeting will be to make initial assessments of damage and assign recovery tasks using the Initial Disaster Recovery Team Meeting Checklist (Appendix E). A Follow-up Recovery Meeting will be scheduled.

CHAPTER 6

CRITERIA FOR ASSESSING THE SITUATION

This chapter defines the criteria that will be used in assessing a situation to determine what scale of disaster should be declared and the tasks that must be activated depending on the severity of the situation.

The levels of Disaster covered are:

Minor

Major

Catastrophic

6.1. Disaster Recovery Processes and Scenarios

A disaster may create a situation in which data backups are the only surviving University records. It is natural, given the excitement and confusion of an emergency, to overlook the need to safeguard these files.

Copying data backup files and returning the originals to their off-site location must take precedence over all activity once the recovery process has begun.

The decision to declare a Major or Catastrophic Disaster will be taken by the Disaster Recovery Coordinator after assessing the situation. It is assumed that the situation will be classified as a disaster if it meets the criteria defined in the following sections (i.e. Minor Disaster, Major Disaster, and Catastrophic Disaster).

If the Disaster Recovery Coordinator decides to initiate Disaster Recovery procedures, all members of Disaster Recovery Teams will follow the procedures contained in this document until the recovery is complete.

The process of recovery following a disaster involves three (3) phases:

1. The initial response from Management
2. Implementation of this Contingency Plan
3. Restoration of normal computer operations

Although the three phases occur in every recovery situation, the activities and the people involved vary according to the nature and severity of the situation.

The following sections identify key activities that will be activated depending on the scale of the disaster.

6.2. Minor Disaster

A **Minor Disaster** is defined as an event that partially interrupts the services provided by the Data Center. Restoration of normal services following a Minor Disaster will generally be within 4 hours but could extend to 2 business days.

Examples of Minor Disasters are:

- _ Miscellaneous Computer or Network Hardware Failure
- _ Data Corruption
- _ System Failure (Computer Software)

Minor disasters are catered for through the concepts and technologies implemented in the Data Center. Some of the recovery methods are transparent to the general user-community, or may affect a select number of individual users.

6.3. Major Disaster

A **Major Disaster** is defined as any event which could result in services supplied by the Data Center being interrupted for a period of time in excess of 2 business days but does not involve the Data Center being destroyed or computer equipment damaged beyond repair.

Examples of Major Disasters are:

- _ Data Center's electrical wiring completely destroyed (water, fire, electrical short circuit, etc.)
- _ Data Center's equipment partially disabled but repairable by vendor field engineers or LSSU employees (water, fire, electrical short circuit, mechanical, etc.)

6.4. Catastrophic Disaster

A **Catastrophic Disaster** is defined as any event which could result in Data Center Services being interrupted for a period of time in excess of 2 business days and may involve the Data Center being completely destroyed.

Examples of Catastrophic Disasters are:

- _ Data Center's major component equipment destroyed (fire, etc) but Data Center physically intact
- _ Data Center completely destroyed (fire, etc)

CHAPTER 7

DISASTER RECOVERY TEAM STRUCTURES AND RESPONSIBILITIES

Team Structures and Responsibilities

The Disaster Recovery Coordinator is responsible for deciding if the situation warrants the declaration of a Major or Catastrophic Disaster.

When a Major or Catastrophic Disaster is declared the organizations defined in this section come into force and generally supersedes any current management structure for the duration of the disaster.

The Recovery Teams will include, but not necessarily be limited to, the following:

- Disaster historian
- Network Recovery Team
- Operations Recovery Team
- Systems Recovery Team

The following sections define the Charter and Responsibilities of the Disaster Recovery Coordinator and of each Recovery Team involved in the execution of the Disaster Contingency Plan. Undertaking predefined activities that are specified by the following Charters and Specific Responsibilities fulfills responsibilities. The Initial Disaster Recovery Team Meeting Checklist and Follow-up Disaster Recovery Team Meeting Checklist (Appendices E & F) will be used to initiate the recovery process with other assignments and checklists made as needed.

7.1. Disaster Recovery Coordinator

The Disaster Recovery Coordinator is responsible for providing overall direction of the Data Center recovery operation. The Coordinator ascertains the total extent of the damage, activates the recovery organization and notifies Recovery Team Leaders.

7.1.1. Charter

The Coordinator is totally responsible for:

- Restoration of the Data Center to provide the correct level of operational service to key users
- Management of all the recovery teams and liaison with appropriate users, etc
- Ensuring audit and security control is maintained during recovery from disaster

- Ensuring emergency costs and expenditures are controlled and recorded
- Ensuring proper communication with internal and external parties as to the impact of the Disaster, the recovery status and plans for continued Business operation

7.1.2. Specific Responsibilities

- Ensure staff safety and welfare
- Evaluate the extent of the problem and potential consequences
- Initiate disaster recovery procedures
- Coordinate recovery teams
- Inform the President of the recovery activities
- Liaison with user management
- Monitor recovery operations and assure schedule accomplishment
- Negotiate with vendors
- Expedite authorization of expenditures by recovery teams
- Ensure all recovery operations are documented by each recovery team
- Record emergency extraordinary costs
- Ensure a detailed accounting of damage is performed to aid in insurance claims
- Ensure computer security standards are adequately monitored
- Name replacements to fill in for absent or disabled disaster recovery team members
- Assign the Disaster Historian responsibility

7.2. Disaster Historian

The Disaster Historian is responsible for establishing and maintaining a record of all disaster recovery activities. This history will be a record of events for subsequent reviews and debriefings with government agencies, insurance companies, vendors, and suppliers. In addition, the Historian will assist by documenting the analysis and conclusions of various Recovery Teams and other interested personnel during and after the disaster. The Disaster Recovery Coordinator will appoint the Disaster Historian.

7.2.1. Specific Responsibilities

The History shall include:

- A chronological log of disaster events
- A chronological log of recovery steps
- Analysis of cause of disaster

- Hours and dollars expended by recovery tasks
- Conclusions with respect to ways in which the interruptions and/or cost could have been reduced
- Recommendations to minimize impacts of a future disaster

7.3. Network Recovery Team

The Network Recovery Team is responsible for establishing a minimum computer network and telephone network to support critical users.

7.3.1. Charter

The Network Recovery Team is totally responsible for:

- Ordering (if necessary) computer network hardware to support critical users
- Supplying and setting up appropriate network software
- Installing a minimum voice network to link Data Center personnel with key users
- Providing appropriate staffing

7.3.2. Specific Responsibilities

- Determine extent of damage to the voice and data networks and initiate repairs
- Order replacement hardware
- Setup a minimum data network and voice network to link Data Center or standby facility with key users
- Provide sufficient personnel to support network repairs
- Reconfigure standby equipment, if required (Appendices G and H)
- Generate and test the network prior to hand-over to Operations Recovery Team
- Manage the network to meet user requirements
- Assist with negotiations with vendors

7.4. Operations Recovery Team

The Operations Recovery Team is responsible for establishing minimum computer processing capabilities to support critical users.

7.4.1. Charter

- Ordering (if necessary) computer hardware for both the standby facility and the main Data Center
- Restoring an up-to-date computer software environment
- Providing appropriate management and staffing of the standby Data Center in order to meet minimum level of user-requirements

7.4.2. Specific Responsibilities

- Determine the extent of equipment usability
- Order replacement hardware
- Notify operations personnel of required activities, locations and schedules
- Setup a working environment on the computing equipment at the standby facility in conjunction with the Systems Recovery Team and Network Recovery Team
- Oversee and coordinate all interim operation functions and equipment recovery
- Provide sufficient personnel to support computer operations at the standby facility
- Obtain all necessary backup material from offsite storage
- Reconfigure standby equipment, if required (Appendices G and H)
- Supervise systems generation and test prior to hand-over to the Systems Recovery Team
- Schedule and direct return to normal processing
- Initiate computer operations at the standby facility
- Manage the standby facility to meet user requirements
- Establish Tape Library functions at the standby facility
- Provide ongoing technical support at the standby facility
- Assist with negotiations with vendors

7.4.3. Additional Tasks

- Establish processing schedule and inform user contacts
- Arrange all necessary supplies
- Reassemble and secure all applicable documentation at the standby facility

7.5. Systems Recovery Team

7.5.1. Charter

The Systems Recovery Team is totally responsible for:

- Supporting operable versions of all critical applications and process systems needed to satisfy the minimum operating requirements
- Providing support for all critical applications and process systems at the standby facility

7.5.2. Specific Responsibilities

- Work with the Operations Recovery Team in reestablishing software and procedure libraries
- Work with the Operations Recovery Team in reestablishing databases to the last backups, and where applicable, journal-file restoration
- Coordinate the various User Groups to aid the recovery of any non-recoverable data
- Supervise the testing and resumption of critical processing
- Run audit tests on the application systems which are processed, shortly after transfer to the standby facility and after transfer back to the main Data Center
- Perform a detailed audit review of the critical files after the first production cycle has been completed
- Inform Operations Recovery Team of backup files needed
- Provide technical assistance to Operations Recovery Team
- Oversee and coordinate all interim systems and programming functions and systems recovery
- Schedule and direct return to normal operations

CHAPTER 8

DISASTER CONTINGENCY PLAN REVISIONS AND TESTING

8.1. Revisions

At the direction of the Disaster Recovery Coordinator the Disaster Recovery Plan will be reviewed every year. Revisions of names, phone numbers, procedures, and equipment will be made and a revised Plan will be distributed.

8.2. Testing

At the direction of the Disaster Recovery Coordinator at least once every 2 years a disaster will be simulated to test the Disaster Recovery Plan by running priority applications in parallel mode on a backup system.

At least once each academic semester one specific SCT application (ADS, FRS, HRS, LMS, or SIS) will be tested by Computer Operations to simulate applicable nightly processing on a backup computer system. A memo stating the scope of testing and the results will be sent to the Disaster Recovery Coordinator and each Recovery Team Leader.

Computer Operations and the appropriate system analyst to simulate applicable nightly processing and online inquiry/update processing will test each time there is a VMS operating system upgrade, one SCT application. A memo stating the scope of testing and results will be authored by test participants and sent to the Disaster Recovery Coordinator and each Recovery Team Leader.

Each time there is installation of a major upgrade to an SCT application, Computer Operations and the appropriate system analyst to simulate applicable nightly processing and online inquiry/update processing will test the application. A memo stating the scope of testing and results will be authored by test participants and sent to the Disaster Recovery Coordinator and each Recovery Team Leader.

Each time there is installation of a major upgrade to the SCT ZSS system, Computer Operations and the appropriate system analyst to simulate online inquiry/update processing will test one SCT application. A memo stating the scope of testing and results will be authored by test participants and sent to the Disaster Recovery Coordinator and each Recovery Team Leader.

Appendix A

Emergency Call List/Disaster Team Leaders

In the event of a disaster the following people are to be notified immediately in the sequence in which they are listed:

1. LSSU Security 635-2210
2. Dr Omer Prewett (Disaster Recovery Coordinator) . . 635-6805
3. Jerry Stephens (Operations Recovery Team Leader). . 632-4382
4. George Rye (Systems Recovery Team Leader) 647-2216
5. Scott Olson (Network Recovery Team Leader). 632-2402

In the event it is necessary to provide notification of a disaster during a period when the Data Center is unoccupied, it is expected that a Security Officer will initiate the notification procedures outlined above until one team member is contacted. The team member notified by Security will complete the notification process.

APPENDIX B

COMPUTER VENDOR AND GENERAL SERVICES PHONE LIST

Computer Vendors and Addresses:

Digital Equipment Corp
800-354-9000 Hardware/Software
Serial # AG02414017
Access # 82710

National Computer Resources, Incorporated
1324 Goldsmith
Plymouth, MI 48170
Contact Person: David Steinhauer
800-686-6274

Emergency and General Service Phone List

On-campus		
Service	Department	Phone
Air Conditioning	Physical Plant	x2372
Equipment Purchases	Purchasing	x2626
Keys	Physical Plant	x2372
Personnel	Human Resources	x2213
Physical Plant	Physical Plant	x2371
Security (Campus)	Security	x2210
Off-campus		
Ambulance		632-2226
Fire		632-3344
Hospital		635-4460
Police - City		632-2216

APPENDIX C

SOFTWARE, FORMS, DOCUMENTATION , ETC. STORED OFFSITE

Application software

All administrative application software is stored on each applicable computers' disk drives.

AlphaServer 2100

Application software is backed up to magnetic tape cartridges every Monday through Friday, utilizing DEC storage system software. Information about the magnetic cartridge backups is stored in the storage system software database, which automatically updates data file creation dates and expiration dates, and tracks the physical cartridges involved. Each morning, the magnetic tape cartridge backups are moved off-site for two business days to a fireproof file box located in Campus Security Office located in the Administration Building, at which time the oldest business day's tapes are returned.

AlphaServer 1000

Application software is backed up to magnetic tape cartridge only as requested.

System Software (Operating system, utilities)

AlphaServer 2100

The system disk pack, which houses the Open VMS operating system and all system utilities being utilized, is backed up once each week to magnetic cartridge. The backup is performed after the nightly processing is completed, but the day of the week may vary. The following morning, the backup volume is moved to a fireproof file box located in the Campus Security Office located in the Administration Building, and the previous week's backup is returned.

AlphaServer 1000

This system pack is also backed up weekly to magnetic tape cartridge typically during the course of normal business hours.

Operations Room Personal Computer

The PC in the operations room is used to provide access to the AlphaServer 2100, AlphaServer 1000, and the Network. Throughout the course of normal operation, files are copied from the Network to the AlphaServer 2100, and vice versa. As such, this PC is critical to the computer operations nightly processing. The PC is equipped with a backup tape drive, and is backed up weekly. These backups are all stored on-site, in a fireproof filing cabinet.

Operating System and System Utility Manuals

Copies of vendor supplied computer operation manuals are kept in the Data Center. It is expected that in a disaster the vendors would expedite delivery of needed manuals

Application Software Manuals

Vendor supplied manuals

A copy of vendor supplied application software manuals is kept in the Administrative Computing area by the system analyst responsible for the applicable system. It is expected that in a disaster the vendor would expedite delivery of needed manuals. Documentation for SCT supplied programs is available for online query from within the applicable system (ADS, FRS, HRS, LMS, SIS).

LSSU authored documentation

Copies of procedures and computer job run streams are stored in the Data Center with an additional copy stored in a locked cabinet in the Leno Pianosi Maintenance Building. LSSU-authored programs and run streams generally contain embedded documentation and comments which are available by viewing via terminal (using an editor) or by printing to a printer.

Preprinted Forms and Stock Paper

Forms and paper supplies sufficient for several weeks processing are stored in the Data Center

The Receiving Department in the Leno Pianosi Maintenance Building has an ample supply of 8.5x11 cut-sheet laser printer paper. It is assumed that local office supply businesses would be able to provide other generic paper quickly, including 14x11 computer paper. Additionally, the agreement LSSU has with Office Depot guarantees next-day delivery of office supplies.

Payroll and Accounts Payable check stock is maintained by the Business Office and is supplied to the Data Center as the Data Center stock is depleted.

Other offices with special forms are required to keep a supply of these forms in their respective areas.

APPENDIX E

INITIAL DISASTER RECOVERY TEAM MEETING CHECKLIST

	Assigned to	Estimated Completion Time	Completed
Assess the nature and extent of the disaster:	_____	_____	_____
- Minor			
- Major			
- Catastrophic			
Assess the status of Data Center:	_____	_____	_____
Contact appropriate officials:	_____	_____	_____
- University President			
- Appropriate Business & Academic Department Heads			
- Physical Plant			
- Digital Equipment			
- Purchasing			
- Insurance			
Report on damage assessment			
- Data Center Usability	_____	_____	_____
- Computer Hardware	_____	_____	_____
- Data Backups	_____	_____	_____
- Software Backups	_____	_____	_____
- Communications	_____	_____	_____
- Security of Center	_____	_____	_____
- Other Facility Contents	_____	_____	_____
- Supplies/Forms	_____	_____	_____
Prepare statement for students and University personnel	_____	_____	_____
Establish time for meeting to report damage assessments w/ recommendations	_____	_____	_____

APPENDIX F

FOLLOW-UP DISASTER RECOVERY TEAM MEETING CHECKLIST

	Recovery Tasks To Be Completed At This Meeting	Complete
1	Obtain & integrate damage assessments	
2	Identify & quantify production capability of the data processing unit that can be available production within a few days with time estimates	
3	Evaluate the need to utilize backup facility	
4	Request production cycle schedule with recommendations of which high priority jobs need to be done	
5	Identify cleanup and repair requirements to support production and start the cleanup and repair	

	Recovery Task To Assign At This Meeting	Assign To:	Complete
1	Assign responsibility for production preparation and startup of production:	Backup software & applications	
		Backup Documentation	
		Supplies and Forms	
		Schedules	
		Technical Support	
		Personnel	
2	Determine the specific requirements for each vendor and assign contact responsibility		
3	Ensure that all data is recorded for history outline		
4	Notify appropriate authorities of extent of disaster and action required		
5	Schedule next recovery meeting		

APPENDIX G

MAINFRAME COMPUTER CONFIGURATIONS

Hardware

Digital AlphaServer Model 2100 (Acquired January 1996)
One 300-Mhz Processor
512-MB memory
Two PCI SCSI controllers (KZPSC-AA), Fast-Wide, RAID capable
One 2.1-GB disk drives
Seven 4.3-GB disk drives

Digital AlphaServer Model 1000 (Acquired January 1996)
One 233-Mhz Processor
128-MB memory
Three 4.3-GB disk drives

Tape Drives

Two TF857 cartridge tape drives, attached to the Model 2100 Server
One TSZ07 9-track tape drive attached to the Model 2100 Server
One TZ86 cartridge tape drive, attached to the Model 1000 Server

Printers

Two LG08 line printers
One LPS17 laser printer
Two LN17 laser printers
One LN14 laser printer

System Software

Digital AlphaServer Model 2100
OpenVMS 6.2
COBOL v2.2
FORTRAN
C++
Storage Library System v2.6
POLYCENTER Scheduler v2.1
POLYCENTER File Optimizer for OpenVMS DFG V2.1A
DECprint Supervisor for OpenVMS v1.1

Digital AlphaServer Model 1000
OpenVMS 7.1
COBOL v2.4

Application Software

Digital AlphaServer Model 2100
Focus v6.9.2
SCT ZSS v1.14
SCT SIS v1.18
SCT FRS v3.0
SCT HRS v4.10
SCT ADS v2.20
SCT LMS v2.00
Resource 25 v1.5

Digital AlphaServer Model 1000

Focus v6.9.2
SCT ZSS v1.14
SCT SIS, FRS, HRS, ADS, and LMS
(These systems may be loaded depending on development requirements)

Security

OpenVMS
SCT ZSS operator number, screen and data element security
SCT value-based security, where provided