

THE UNIVERSITY OF NORTHERN IOWA  
CEDAR FALLS, IA

INFORMATION TECHNOLOGY SERVICES  
**DISASTER RECOVERY PLAN**

LAST UPDATED  
MAY 25, 2000

## TABLE OF CONTENTS

<b>ADMINISTRATIVE SYSTEMS .....</b>	<b>5</b>
GENERAL .....	5
CONCEPT.....	5
DEFINITIONS .....	5
CONTINGENCY COMPUTER SITE.....	6
IMPACT ANALYSIS .....	7
SECURITY .....	7
<i>GENERAL</i> .....	7
<i>CURRIS BUSINESS BUILDING (CBB) FACILITY</i> .....	8
<i>OFF-SITE STORAGE</i> .....	8
<i>SOURCE DOCUMENTS AND DATA FILES</i> .....	9
<i>VITAL RECORDS</i> .....	9
BACKUP PROCEDURES.....	10
MANAGEMENT SUPPORT .....	11
VENDOR INTERFACE .....	11
CAMPUS INTERFACE .....	12
PLAN MAINTENANCE, TESTING, AND APPROVAL.....	12
<b>APPENDIX I.....</b>	<b>14</b>
IBM SITE DISABLED .....	14
GENERAL .....	14
DISASTER ALERT .....	14
<i>MINOR DISASTER</i> .....	14
<i>MAJOR DISASTER</i> .....	14
<i>CATASTROPHIC DISASTER</i> .....	14
DISASTER MANAGEMENT TEAM.....	14
RECOVERY TEAM.....	15
SITE RECONSTRUCTION TEAM .....	15
<i>MINOR DISASTER</i> .....	15
<i>MAJOR DISASTER</i> .....	15
<i>CATASTROPHIC DISASTER</i> .....	15
<i>ITS STAFF</i> .....	16
<i>USER GROUP REPRESENTATIVES</i> .....	17
RECOVERY OPERATIONS CENTER.....	18
<b>ADMINISTRATIVE SYSTEM DISABLED.....</b>	<b>19</b>
RESPONSIBILITIES/ACTIONS.....	19
<i>SENIOR OPERATOR ON DUTY</i> .....	19
<i>IBM SYSTEMS PROGRAMMER</i> .....	19
<i>DEC SYSTEMS ADMINISTRATOR</i> .....	19
<i>UNIX SYSTEMS ADMINISTRATOR</i> .....	20
<i>ASSOCIATE VICE PRESIDENT FOR INFORMATION TECHNOLOGY</i> .....	20

<i>SYSTEMS &amp; OPERATIONS MANAGER</i> .....	20
<i>NETWORK SERVICES DIRECTOR</i> .....	20
<i>USER SERVICES DIRECTOR</i> .....	21
<i>INFORMATION SYSTEMS DIRECTOR</i> .....	21
<i>RECOVERY TEAM</i> .....	21
<i>SITE RECONSTRUCTION TEAM</i> .....	21
EQUIPMENT REQUIREMENTS .....	22
STUDENT COMPUTER CENTER (SCC) FILE SERVERS .....	22
SUPPLY REQUIREMENTS .....	22
<b>ACADEMIC SYSTEM DISABLED</b> .....	<b>23</b>
RESPONSIBILITIES/ACTIONS .....	23
<i>SENIOR OPERATOR ON DUTY</i> .....	23
<i>DEC SYSTEMS ADMINISTRATOR</i> .....	23
<i>UNIX SYSTEMS ADMINISTRATOR</i> .....	23
<i>ASSOCIATE VICE PRESIDENT FOR INFORMATION TECHNOLOGY</i> .....	23
<i>SYSTEMS &amp; OPERATIONS MANAGER</i> .....	24
<i>INFORMATION SYSTEMS DIRECTOR</i> .....	24
<i>NETWORK SERVICES DIRECTOR</i> .....	24
<i>USER SERVICES DIRECTOR</i> .....	25
<i>RECOVERY TEAM</i> .....	25
<i>SITE RECONSTRUCTION TEAM</i> .....	25
EQUIPMENT REQUIREMENTS .....	25
<i>ADMINISTRATIVE HARDWARE</i> .....	26
<i>ADMINISTRATIVE SOFTWARE</i> .....	27
<i>ACADEMIC HARDWARE</i> .....	28
<i>ACADEMIC SOFTWARE</i> .....	30
SUPPLY REQUIREMENTS .....	30
<b>APPENDIX I, ATTACHMENT 1</b> .....	<b>31</b>
ITS CALL IN INFORMATION .....	31
EMERGENCY ALERT ROSTER .....	32
BACKUP ALERT ROSTER .....	32
NETWORK ACTION TEAMS .....	32
<b>APPENDIX I, ATTACHMENT 2</b> .....	<b>35</b>
SUPPLIES CHECKLIST .....	35
<b>APPENDIX I, ATTACHMENT 3</b> .....	<b>36</b>
COMPUTER PRINT FORMS INFORMATION .....	36
VENDORS .....	39
<b>APPENDIX I, ATTACHMENT 4</b> .....	<b>41</b>
ADMINISTRATIVE SYSTEM BACKUP PROCEDURES .....	41
<b>APPENDIX II</b> .....	<b>48</b>

USER REACTION PLANS ..... 48

**APPENDIX III..... 50**

MEMORANDUM OF UNDERSTANDING ALTERNATE SITE PROCESSING ..... 50

**APPENDIX IV..... 52**

SUGGESTED LETTER TO DEPARTMENTS ..... 52

This file is located on Karen Paulsen's PC

(c:\data\disaster recovery\disaster recovery plan 1999.doc)

University of Northern Iowa  
Information Technology Services

ADMINISTRATIVE SYSTEMS  
DISASTER RECOVERY PLAN

## GENERAL

A disaster recovery plan is vital to Information Technology Services' management and campus administration in order to insure continuity of computer operations under emergency or disaster situations. Conditions such as extended computer downtime, natural disasters, or criminal action could require implementation of part or all of the plan. To be effective, the plan must be flexible enough to apply under as many conceivable conditions as possible.

When a disaster occurs, a disaster emergency alert is called notifying key personnel (the Disaster Management Team). These individuals meet, make an assessment of the situation, and under the direction of the Disaster Plan Coordinator, incorporate implementation strategies based upon the severity of the problem and the immediate computational needs of the campus administration.

## CONCEPT

Within the framework of this plan, a disaster is any event which results in an unexpected computer shutdown such that processing must be accomplished at another site for some period of time. The overall plan provides a description of the resources, procedures and decisions required before, during and after such a disaster to insure that the essential daily business and administrative functions of the campus continue in an orderly fashion.

This plan is developed around off-site storage of backup files, and the use of the campus' alternate processing site(s) to carry on critical administrative computing applications. It meets the disaster recovery requirements of a minor or major disaster, as defined below, with the expectation that the primary and alternate processing sites would not both be destroyed in the same disaster occurrence.

## DEFINITIONS

An INTERRUPTION OF COMPUTER SERVICES is defined as a situation in which the central computer system, or some peripheral component, is down and precludes computing for a period of less than 24 hours. No facility damage has occurred. Such an occurrence is normally covered by day-to-day emergency procedures and close coordination with the system vendor and its maintenance personnel. An example would be minor hardware or software problems, a major file reload, or a head crash on a critical disk. In cases where an application is required before the system can be returned to normal operation, some level of recovery action may be required.

A MINOR DISASTER is defined to be one in which the central computer system(s) can be restored to, or nearly to, normal operational capacity within four (4) days, or earlier if there is a critical time by which a particular software application must be run to completion. Examples would be a system down awaiting parts, a minor fire or flood, or perhaps software problems requiring a minor rewrite. Little or no facility damage would have occurred.

A MAJOR DISASTER is defined to be one in which the computer(s) are expected to be down for more than four days, or beyond the time a critical software application must be run to completion. A long-term loss of administrative computing support at the particular site can be expected. A more extensive fire or flood, a small earthquake, or minor terrorist activity or civil disorder could place us in a position where damage is extensive and could require a new facility or replacement of major computer components or entire systems. The campus, itself, would still be in operation and require administrative computer support.

A CATASTROPHIC DISASTER is defined to be one wherein the operation of the entire campus is disrupted, and there would be no need for computer support until rebuilding took place and normal campus activities could begin again. A major earthquake, all encompassing fire, or extensive terrorist bombings are examples of possible causes.

A MUTUAL AID AGREEMENT is defined as an informal reciprocal agreement with a computer site that has similar equipment, in which each party agrees to provide computing facilities to the other to the extent possible to meet the emergency priority processing requirements outlined in the agreement. Under this type of agreement the host's requirements have priority; thus, access to facilities is not guaranteed for any particular time or application, but the host will do its utmost to provide the necessary facilities at the earliest time practical. Although processing time cannot be guaranteed, limited processing can generally be agreed to within some reasonable time frame, such as within 24 hours after request. The only charges incurred under this type of agreement are normal usage charges, if any, when off-site processing is actually accomplished. The MEMORANDUM OF UNDERSTANDING (APPENDIX III), which can be used for an agreement between two sites, will define any charges to be incurred.

A mutual aid agreement generally is satisfactory only under short term circumstances requiring limited processing. Therefore, it is doubtful if administrative computing could continue even on a limited basis for an extended period under mutual aid. With the two computer sites and systems currently available to the campus, this type of agreement is not a necessity.

### **CONTINGENCY COMPUTER SITE**

Since the completion of the Curris Business Building (CBB) and subsequent move of ITS computers into that building in the Summer of 1990, the UNI campus has had contingency sites for computing. The former administrative computer room located in GIL-255 is available as a contingency site(s). Those rooms have false flooring as well as sufficient emergency electrical power and air conditioning that can be used to complete critical functions until the problem is resolved, and either will also serve as an alternate processing site for the other for minor and major disaster situations.

To begin computing again after a long term catastrophic disaster, where the entire campus is destroyed, the campus administration might be required to support the high cost of a contractual arrangement for a full time "cold" backup computer facility for reinitiating all, or nearly all, computational requirements, both administrative and academic. A "cold" site is one in which air conditioning and power are provided, but the user must have their required computer system

installed and operated from that location until their own facilities can be rebuilt. Several companies provide this service for users of large scale IBM and DEC computer systems. The cost is very high, and alternatives would have to be evaluated as recovery from a catastrophic disaster begins.

## **IMPACT ANALYSIS**

Interruption of computing services for any length of time, when those services are expected to be available, is at least an irritation and can very quickly become a major detriment to the functioning of the University. A survey of key users of the administrative computing system on this campus indicates that the time of the month has much to do with the maximum downtime any particular user can sustain without seriously affecting the daily business of the University. For example, payroll processing leaves little time between the beginning of a pay cycle and the time the money is to be available to the employee, either in the form of a check or a direct deposit to a bank. Thus, if one of the pay cycles is about to begin or is in process, any amount of downtime is critical. But otherwise, perhaps as much as a week of downtime could occur with only minor inconvenience, for that office/function.

In general, we can say that on an average we could have the possibility of three or four days of downtime before off-site processing would absolutely have to begin for one or more administrative systems. Each situation must, however, be evaluated based on the circumstances at the time, and the decision made through a coordinated effort by the Disaster Plan Coordinator, representatives of the administrative users, and the Disaster Management Team. The following **PRIORITY ASSIGNMENTS** normally will be adhered to:

<b>PRIORITY</b>	<b>TYPE OF PRODUCT</b>
1	Payroll checks and supporting documents
2	Accounts Payable
3	Student Information Systems
4	Financial reports
5	Other

Temporary **MANUAL PROCESSING** procedures must be developed by each major administrative system, such as identified in 1 through 4 above. The specific details must identify the manual procedures to be followed, who is to implement those procedures, and the direct costs and intangible risks of both manual and alternate site processing. These details will be outlined in a **USER REACTION PLAN (APPENDIX II)** developed by the administrative department responsible for the data, and will be coordinated with the Associate Vice President for Information Technology.

## **SECURITY**

### GENERAL

In the event of a disaster, both the Cedar Falls Fire Department and Police Departments will be notified of the situation, and appropriate action initiated. Ongoing security arrangements in a disaster situation will be coordinated with the Campus Public Safety Office.

## CURRIS BUSINESS BUILDING (CBB) FACILITY

The IBM 9672-R12 administrative computer is located in the main computer room, room 19, in the first floor of CBB. Only limited access is allowed to the facility (Operations, Telecommunications and Systems personnel). Fire alarm is in the hall, next to the double door to the ITS pickup room. Hand held fire extinguisher(s) are also readily available.

## OFF-SITE STORAGE

"Off-site" in this sense refers to a fire rated security vault located in the main computer room, and to one or more locations in facilities other than the CBB complex, as well as locations off the UNI main campus. Off-site storage is used to help assure a backup file source in the event that files located within the Center are destroyed. Off-site storage requires a controlled environment, a means to insure the security of the files, and ready accessibility.

On campus, four locations meet these requirements. They are the ITS safe located in CBB-19, the fire-proof cabinets in CBB-19, the locking storage cabinets in GIL-1, and the safe located in the Controller area in GIL-256. The ITS safe is a Class 150 fire rated for two hours. It will hold as many as 274 tapes. The Controller's area is used to store production campus payroll and accounts payable check blanks. The Controller safe is fire rated at 2000 degrees Fahrenheit for four hours to maintain internal temperature at or below 150 degrees and humidity at or below 85%.

Off-campus storage is supplied by contract with FirStar Bank of Cedar Falls, IA. Backup tapes of the administrative systems are taken to the bank on weekly and monthly cycles and the tapes from the previous week/month are returned to the UNI Center at CBB.

Disaster security of administrative files is the responsibility of the Information Systems (IS) unit, and is provided by using the remote storage facilities of FirStar Bank. Copies of critical current and historical files, as identified by IS in conjunction with the users, are removed from the Center on a monthly basis and stored off-site in environmentally controlled vaults. Magnetic tape copies of all on-line administrative disk packs are likewise secured. The most recent cycle of backups is kept on-site in the ITS safe, and earlier versions are maintained at FirStar Bank for a month. As part of the contract service, in an emergency, these files can be retrieved at any time within two hours of notification.

Administrative users desiring off-site backup storage must coordinate their needs through ITS. ITS will maintain an inventory of all administrative backup tapes stored off-site.

All other users desiring off-site backup to their files must coordinate their needs through ITS Systems and Operations at the counter in the CBB Center. Tapes will be stored within the campus facilities or under contract with FirStar Bank as needs dictate. Systems and Operations will maintain an inventory of all system backup tapes stored off-site. The following indicates system security password information:

IBM: Four persons are given "system special" privileges via OS/390 1.2 Security Server (RACF 2.2.0). The older methods of maintaining a password dataset, and password

protecting the master catalog, are no longer used. A small SYS1.UADS is maintained in the unlikely event that RACF is not available. Two TSO users are defined via SYS1.UADS.

Sun: The passwords for root accounts will be placed in a sealed envelope.

VMS: The password for SYSTEM will be placed in a sealed envelope.

All three envelopes will be placed in a safe deposit box (#362) at FirStar Bank secured for this purpose. There are two keys to the safe deposit box, one is located in Ken Connelly's locked file cabinet in his office in CBB 15. A second key is kept in a red envelope within the wall mounted key cabinet in the GIL 255 office area. The signature card for the box will include ITS personnel; Steve Moon, Ken Connelly, Randall Maas, Keith Young, Kevan Forest; Wayne Ostendorf, Director, ADP, Iowa State University; Darlyn Sawin, Director, ADP, University of Iowa.

#### SOURCE DOCUMENTS AND DATA FILES

Information Systems (IS) is responsible for the source data files and documentation of the administrative systems under their control. Other individual users are responsible for their own systems.

The IBM, DEC and SUN system source files and documentation are the responsibility of the ITS Network Services unit.

#### VITAL RECORDS

Vital records are those which are necessary for the reconstruction and ongoing operation of the campus administrative activities and administrative computing functions. These records must be identified by the individual departments and duplicate storage sites used to assure their retrieval. Departments must provide an inventory of their vital records, and their location in their User Reaction Plan, which becomes part of APPENDIX II of the Disaster Recovery Plan. For those units under the Director of Information Technology Services, the alternate storage site will be in the FirStar Bank.

## **BACKUP PROCEDURES**

The IBM system files are copied to cartridge tape every night during the full volume backups of the entire production LPAR DASD farm. The latest nightly copy is stored in the safe, the latest weekly copy is retained by FirStar Bank.

The files for administrative systems are backed up as follows (generally at end of business hours on-line system shutdown and again nightly after batch processing):

STUDENT databases are copied to tape after every update cycle.

PAYROLL databases are copied to tape after every update cycle.

GENERAL LEDGER databases are copied to tape after every update cycle.

ACCOUNTS PAYABLE databases are copied to tape after every update cycle.

MISCELLANEOUS systems (Human Resources, Physical Plant, Equipment Inventory, Public Safety, Campus Directories, Residence, etc.) databases are copied to tape after every update cycle.

In addition to the backup of major files as noted above, all files on the IBM system disks are copied nightly and kept. Each Tuesday, the cycle become the "weekly" backup, and is stored in the vault at FirStar Bank until replaced by the next weekly set. Once each month, in place of a "nightly" backup, a "monthly" backup is produced and stored in the vault at FirStar Bank until replaced by the next monthly set. Additionally, backups are also kept of calendar year end, fiscal year end (June 30) closing, and other user designated intervals as identified by users. User data information is retained as designated/requested.

COMPLETE IMAGE BACKUPS FOR DEC files are created at the end of each week. The weekly backup that covers the last day of the previous month is defined as a "monthly" backup. Weekly backups are retained for one month, monthly backups are retained for one year. The May and December backups are retained indefinitely.

BACKUP OF ALL SUN file systems is done monthly. Incremental backups are done daily between each monthly system backup. Monthly tapes are archived for one year and are stored on-site in the CBB 19 fireproof data safe.

All ITS MANAGED NOVELL AND NT FILE SERVERS are backed daily so that daily, weekly, and monthly versions of both system and user volumes is available. Monthly versions are kept for 1 year and stored in off-site and off-campus locations. The previous two monthly backups are kept off-campus at FirStar Bank and the ten months prior to those backups are kept off-site in the CBB 19 fireproof cabinet storage. Systems diskettes and configuration details are stored in an off-site location. Non-ITS managed servers connected to UNI-Net can elect this backup service.

The DATA ENTRY BACKUP SITES are the responsibility of the individual user offices as this function/responsibility is distributed.

The TELEPHONE SWITCH/VOICE MESSAGING SYSTEM are backed up on a tape every day. If the switch/voice messaging system should lose memory for any reason, the backup tape

automatically reloads the software to memory. Periodically, these tapes are copied, with one set of copies located in the GIL 38 Switchroom and one set of copies kept in the ITS fireproof vault.

Presently, there are six telephone switch nodes throughout campus. Each node is connected to a UPS which provides 15-30 minutes of uptime (depending on switch load). In addition, each node (except ROTH) is on the UNI emergency generator system, to provide continuous power in the event of main power failure. Physical Plant performs periodic tests on the generator system.

### **MANAGEMENT SUPPORT**

It is extremely important that this plan is reviewed and fully supported by the campus management. There must be a firm agreement on which applications are critical, and the priority in which they will be processed at our alternate site.

A USER REACTION PLAN (UREACT) must be in place and tested for each critical business application. These plans must be designed to provide specific guidelines for the actions to be taken by the user group when the computer is down for an extended period. Critical operations and the time frame in which they become critical must be defined. These plans are independent of the master Disaster Recovery Plan, but must be coordinated directly with the master plan so that all involved are fully aware of the particular needs and what must be done to meet those needs. The requirement for specific departments to develop User Reaction Plans and the procedures to implement them is directed by the Vice President for Administration and Finance. These plans must be approved by the Director of Information Technology Services and Internal Audit. Copies of these User Reaction Plans will be appended to this master plan as attachments to APPENDIX II.

### **VENDOR INTERFACE**

The appropriate vendor (presently SUN, DEC, Cabletron, Compaq, and IBM) will be notified of all disaster situations so that full maintenance support can be had at the earliest possible time. There very well could be the need for immediate negotiations concerning computer time and services, replacement hardware, and temporary site relocation, when extensive or total rebuilding is necessary.

Vendors for other equipment and supplies, such as communications, air conditioning, power conditioning, tapes, and even facility designer/builders, will be notified as necessary. The Director of Network Services will maintain records of existing vendor contracts and files of vendors of potential needs. Normal Campus Policies and Procedures will be used in all acquisitions, but with an emergency priority.

#### **SUN CONTACT**

Sun Microsystems Computer Corporation  
Minnesota Center, Suite 950  
7760 France Avenue South  
Bloomington, MN 55435  
612-832-4120  
Dorothy Hruska

#### **DEC CONTACT**

**DEC**

Attn: Tim Houston  
100 Northwest Point Boulevard  
Elk Grove Village, IL 60007-1018  
(708) 806-0200

**CABLETRON**

Cabletron  
Attn: Randy Coffey  
3620 Twana Drive #18  
Des Moines, IA 50310  
(515) 276-3380

**COMPAQ**

Entre Computer Center  
Attn: Brad Miller  
1850 Boyson Road  
Hiawatha, IA 52233  
(800) 795-2630

**IBM CONTACT**

International Business Machines  
Attn: Mike Bourgo, Marketing Manager  
1901 Broadway Street  
Iowa City, IA 52240  
Internet: MBBOURG@CHGVMIC1.VNET.IBM.COM  
(800) 765-8799 extension 6501

**CAMPUS INTERFACE**

Public Safety, Physical Plant, and other appropriate departments will be notified, as necessary, of disaster situations requiring their assistance and support.

Human Resource Services will be notified immediately if there is a need to hire temporary or full time personnel because of a disaster. Normal Campus Policies and Procedures will be used in all hires, but with an emergency priority.

**PLAN MAINTENANCE, TESTING, AND APPROVAL**

The Associate Vice President for Information Technology must approve this plan and all subsequent changes or addenda to it. The plan will be reviewed at least annually for adequacy under the operational requirements at that time. Off-site storage contracts will be renewed annually. An updated equipment list must be provided at the time of any change, and should be reviewed for accuracy during periodic tests of the disaster plan. Mutual aid agreements, if necessary, will be renewed annually, or as established in the agreement, and include an updated equipment list.

After each test, the Disaster Management Team will brief management on the test, with emphasis on those areas where problems occurred, and make recommendations for improving the plan. Suggested changes to this plan should be brought to the attention of the Associate Vice President for Information Technology.

This plan is approved with the changes incorporated as of the date signed.

\_\_\_\_\_ *signature on file* \_\_\_\_\_  
Garry Bozylinsky  
Associate Vice President  
Information Technology Services

\_\_\_\_\_ Date

APPENDIX I  
DISASTER RECOVERY PROCEDURES

**IBM SITE DISABLED**

**GENERAL**

These procedures will be implemented any time a minor or major disaster occurs at the IBM site causing a situation wherein processing of administrative applications must be moved to the GIL-255, or where the GIL-255 site is also damaged and administrative applications must be moved to the BAK-11 location.

**DISASTER ALERT**

Upon the occurrence of any disaster situation, the senior operator on duty will notify the Campus Public Safety, and the ITS Systems and Operations Manager as part of the normal emergency alerting procedures. The Systems and Operations Manager at the site involved in the disaster will make an immediate assessment of the situation to the best of their ability, notify the Disaster Plan Coordinator, and call the vendor for maintenance support, as necessary. See Attachment 1, "Emergency Alert Roster," (and Appendix I, Attachment 1, "Backup Alert Roster, when necessary) for names and numbers.

**MINOR DISASTER**

The Disaster Plan Coordinator and the Systems and Operations Manager will determine whether or not the extent of the disaster is sufficient to warrant the assembly of the Disaster Management Team. If not, recovery operations will be accomplished by the Systems and Operations Manager in accordance with normal emergency procedures.

**MAJOR DISASTER**

After determining the extent of the disaster, the Disaster Plan Coordinator will assemble the Disaster Management Team using the Emergency Alert Roster, APPENDIX I, Attachment 1.

**CATASTROPHIC DISASTER**

The Disaster Plan Coordinator will assemble the Disaster Management Team when communications have been reestablished and a plan for campus recovery has been enacted by the administrative officials of the campus.

**DISASTER MANAGEMENT TEAM**

The Disaster Plan Coordinator will notify the Disaster Management Team (as required) to gather at the designated location as soon as possible after notification of a disaster. Normally this location will be at the ITS CBB-15 conference room, but an alternate conference room will be made available to use, if necessary, through coordination with Campus Planning. The team will consist of the following members:

- Associate Vice President for Information Technology (Disaster Plan Coordinator)
- Systems & Operations Manager

- Information Systems Director
- Network Services Director
- User Services Director

### **RECOVERY TEAM**

The Recovery Team will be called together, as necessary, by the directors in the Disaster Management Team. The team will consist of the following members, as required by the nature of the disaster:

- Information Systems Director (Recovery Team Leader)
- Systems & Operations Manager
- Computer Operator(s)
- Systems Programmer(s)
- Voice Services Manager/Communications Specialist
- Others, as deemed necessary by the circumstances

### **SITE RECONSTRUCTION TEAM**

The Site Reconstruction Team, if necessary, will be called together by the Disaster Management Team as soon as practical following the disaster. Team members and number will vary according to the nature of the reconstruction effort. Minimum members will be:

#### **MINOR DISASTER**

- Systems & Operations Manager
- Information Systems Director
- Information Systems Managers

#### **MAJOR DISASTER**

- Disaster Management Team
- Planning Architects
- Physical Plant Engineers Representative
- Public Safety Representative
- Vendor Representative(s)
- User Group Representatives
- Others, as required

#### **CATASTROPHIC DISASTER**

The Disaster Plan Coordinator will be notified by Public Safety as to when to meet and who needs to be involved. The Disaster Management Team should be expecting notification once communications are reestablished following a catastrophic disaster.

The following is a telephone list of ITS staff and User Group Representatives:

### ITS STAFF

<b>Name</b>	<b>Title</b>	<b>Phone #</b>	<b>Pager #</b>
Bergstrom, Pat	Telecommunications Operator	32271	
Berning, Barb	Data Technician III	36820	
Bozylinsky, Garry	Associate Vice President	37779	
Brasch, Sandra	Support Services Coordinator	32427	
Bull, Troy	Senior Programmer Analyst	37430	
Case, Doug	LAN Specialist	37145	Pager 236-6209
Clopton, Neil	Personal Workstation Specialist	37216	
Connelly, Ken	Systems & Operations Manager	35850	Pager 833-4170
Cooper, Vergestene	Data Technician III	36818	
Cue, Connie	Systems Analyst	32042	
Daley, Maureen	Systems Analyst	32415	
Drachenberg, Sharon	Telecommunications Specialist I	32436	
Fisher, Jeanie	Senior Programmer Analyst	35822	
Forest, Kevan	Database Administrator	32453	
Fox, Bobbie	Senior Programmer Analyst	32445	
Fritts, Jane	Secretary II	37076	
Goro, Terry	Coordinator of Instructional Technology Services	35853	
Griffin, Joleen	Electronics Technician II	32436	Pager 236-6026
Hall, Kevin	External Services Systems Integrator	36941	
Hausmann, Mary Ann	Programmer Analyst	32434	
Hayek, Doreen	Special Projects Administrator	37300	
Hayes, Randy	Voice Services Manager	37473	Pager 235-8664
Hayungs, D. Todd	Ed Technology Engineer	36292	
Heiple, Julie	Data Access Administrator	37431	
Hendrickson, Sandra	Coordinator Graphics and Courseware Production	36140	
Hetrick, Bob	WAN Specialist	32961	Pager 236-6028
Hibbard, Philip	Ed Technology Specialist	37197	
Hobkirk, Eunice	Secretary III	37607	
Johnson, Betty	Secretary III	37133	
Johnson, Dennis	Senior Programmer Analyst	37143	
Jongedyk, Holly	Programmer Analyst	37874	
Kacmarynski, David	CIS Technician II	37636	
Lawin, Gene	Computer Network Systems Manager	32947	Pager 235-4070
Lerner, Galina	Programmer Analyst	36982	
Lindner, Dennis	Director, Information Systems	32424	
Luck, Clyde	Data Systems Coordinator	32289	
Maas, Randy	Senior Systems Programmer/IBM	33001	
Marchesani, Joseph	Asst Prof/Coord TV/Audio	36292	
Miller, Jack	Consulting Center Manager	35943	
Mixdorf, Jim	CIS Technician II	37637	
Moon, Steve	Director, Network Services	36813	
Morehead, TyAnn	Ed Technology Specialist	35854	
Morgan, Aaron	Electronics Technician II	32871	Pager 236-6030
Mundhenke, Monica	Information Systems Manager	36146	
Nelson, Dan	Residential Network Specialist	37423	
Palmersheim, Pat	Database Analyst	36162	
Patterson, Denise	CIS Technician I	37638	
Paulsen, Karen	Secretary IV	36815	
Perry, Donald	Clerk IV	32342	
Peterson, Tom	Director, User Services	36460	
Pugh, Emrys	Senior TV Engineer	36294	
Quarnstrom, Kevin	Information Systems Manager	32444	

Rasmussen, Lyle	Information Systems Manager	32430
Reimer, Dennis	Coordinator of Multimedia Distribution	36285
Richter, Laura	Systems Analyst	35821
Rooff, Tricia	Programmer Analyst	37141
Schauls, Mark	Senior Programmer Analyst	32531
Schultz, Judy	Sr Systems Programmer/Sr Programmer Analyst	36816
Seeley, Richard	Coordinator of Multimedia Conferencing	37218
Sherbet, Boyd	ICN Scheduler	37188
Sullivan, Diane	Support Services Manager	36814 Pager 236-6041
Teramoto, Yayoi	Programmer Analyst	36983
Thompson Yezek, Peter	Web Tools Specialist	37390
Triplett, Andy	Data Network Assistant	37851
Turner, Valerie	Programmer Analyst	37606
Van Pelt, Darlene	Programmer Analyst	32409
Westendorf, Mary	Systems Analyst	32403
Wolter, Jon	Field Services Manager	36834 Pager 236-6027
Young, Keith	Senior Systems Programmer/UNIX	32008

### USER GROUP REPRESENTATIVES

<b>Name</b>	<b>Department</b>	<b>Office Phone</b>
Clark Elmer	Admissions	32281
Mark Renner	Admissions	32281
William Calhoun	Alumni	36078
Michael Hoy	Alumni	37110
Scott Leisinger	Athletics	36078
Julie Bright	Athletics	32475
Eunice Dell	Budget	32383
Mary Prenosil	Budget	36137
Gary Shontz	Controller	33576
Bruce Rieks	Controller	33544
Roland Carrillo	Financial Aid	32701
Sam Barr	Financial Aid	32701
Eileen Dams	HRS	33425
Nick Bambach	HRS	32242
Dean Shoars	Physical Plant	32712
David Anderson	Physical Plant	35923
Dennis Hayes	Physical Plant	37653
Muriel Stone	Placement	32083
Morris Mickelson	Planning	36181
George Pavelonis	Planning	36181
Bob Wyatt	Planning Admin.	36385
Susan Chilcott	Public Relations	32761
Vicki Grimes	Public Relations	32761
Dean Shoars	Public Safety	32582
David Zarifis	Public Safety	32712
Roxeanne Conrad	Purchasing	33524
Chuck Neil	Purchasing	32980
Phil Patton	Registrar	32283
Patti Rust	Registrar	32113
Doug Koschmeder	Registrar	32112

## **RECOVERY OPERATIONS CENTER**

The Disaster Plan Coordinator (DPC) will establish a Recovery Operations Center (ROC) as soon as possible after convening the Disaster Management Team. The ROC normally will be located at the ITS CBB-15 conference room (Phone: 273-6814), but the nature of the disaster may require another location. GIL-255, GIL-209 and the UNI-Dome facility are other potential locations, if necessary. Once established, the ROC will be operational on a 24-hour basis until de-escalation is appropriate and directed by the DPC.

The following items should be available at the ROC:

- Two or more telephone lines
- Phone log
- Telephone directories (Campus & Cedar Falls-Waterloo)
- "Status" board (blackboard, whiteboard, etc.)
- Recovery Plan manuals
- Portable battery operated radio
- Portable battery operated tape recorder
- Six 60-min or four 90-min cassettes
- Battery operated clock
- University Credit cards
- Cash (\$50 - \$100 petty cash)
- First aid supplies
- Food, dehydrated (for six people for two days)
- Water (for six people for two days)
- Personal care items (e.g., soap, towels, etc.)

## ADMINISTRATIVE SYSTEM DISABLED

### **RESPONSIBILITIES/ACTIONS**

#### SENIOR OPERATOR ON DUTY

- Notify Public Safety and Cedar Falls Fire Department, as the situation dictates.
- Notify the Systems & Operations Manager of the event and the current status.
- Verify Current Nightly Backups are locked in ITS safe.
- Perform system shutdown and other emergency procedures, and/or evacuate the facility, if necessary.

#### IBM SYSTEMS PROGRAMMER

- Determine the extent of the disaster to personnel, equipment, facility and operational capability.
- Provide data to assist Associate Vice President for Information Technology in identifying the time and place to convene the Disaster Management Team.
- Notify the Information Systems Director of the event, and to continue the alert roster and convene the Disaster Management Team.
- Notify the vendor(s) for maintenance support.
- Identify what, if any, functions can continue on-site.
- Collect system backup tapes or retrieve from FirStar Bank.
- Assemble vital documents, or retrieve from off-site location.
- Meet with the Disaster Management Team at the time/place designated.
- Provide a schedule of operators.
- Identify and notify operator(s) for Recovery Team.
- Coordinate processing priorities with the appropriate IS teams.
- Gather necessary equipment and supplies, e.g., tapes, paper, and special forms (see Appendix I, Attachment 3, "Supplies Checklist").
- Arrange transportation.

#### DEC SYSTEMS ADMINISTRATOR

- Notify the Systems & Operations Manager to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Provide a schedule of operators.
- Coordinate processing priorities with the DEC users.
- Gather necessary equipment and supplies, (see Appendix I, Attachment 2, "Supplies Checklist").

### UNIX SYSTEMS ADMINISTRATOR

- Notify the Systems & Operations Manager to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Provide a schedule of operators.
- Coordinate processing priorities with the SUN users.
- Gather necessary equipment and supplies, (see Appendix I, Attachment 2, "Supplies Checklist").

### ASSOCIATE VICE PRESIDENT FOR INFORMATION TECHNOLOGY

(Disaster Plan Coordinator)

If a minor disaster:

- Determine whether or not to assemble the Disaster Management Team (DMT).

If the DMT is to be assembled:

- Meet with the Disaster Management Team at the time/place designated.
- When the team is assembled, determine expected processing needs.
- Establish processing priorities and scheduling requirements.
- Assemble and brief the Recovery Team, as necessary.
- Document actions.

For major and catastrophic disasters, also:

- Establish a Recovery Operations Center (ROC) for coordination of all recovery activities.
- Schedule personnel to staff the ROC.
- Establish escalation/de-escalation plans.
- Assemble and brief the Site Reconstruction Team.

### SYSTEMS & OPERATIONS MANAGER

- Notify the Network Services Director to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Coordinate any system programming requirements.
- Collect production backup tapes or retrieve from FirStar Bank or have FirStar Bank deliver to the recovery site, as applicable.
- Provide a schedule of system programmers.
- Identify and notify system programmer for Recovery Team.

### NETWORK SERVICES DIRECTOR

- Notify the User Services Director to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Determine which critical applications are dependent upon data communications and what can be done (on-line systems).
- Establish required communications.

- Coordinate communications requirements.
- Provide a schedule of communications personnel.
- Identify and notify communications specialist for Recovery Team.

#### USER SERVICES DIRECTOR

- Notify the Information Systems Director to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Notify users of the level of service available.
- Determine administrative processing needs during expected down time.
- Coordinate priorities and establish a processing schedule.
- Provide a schedule of User Services personnel.
- Identify and notify the User Services individual who will be a member of the Recovery Team.
- Coordinate communication between user community and Recovery Team.
- Provide for distribution of administrative documents.

For major and catastrophic disasters:

- Notify administrative users of the ROC location and telephone number, and the distribution point for processed documents.

#### INFORMATION SYSTEMS DIRECTOR

- Meet with the Disaster Management Team at the time/place designated.
- Notify users of extent of the disaster and direct them to implement their User Reaction Plan (UREACT).
- Provide the team with a schedule of administrative programmers.
- Identify and notify programmer(s) for Recovery Team.

#### RECOVERY TEAM

- Meet with the Disaster Management Team at the time/place designated.
- Proceed to recovery site location with required software, equipment, documentation, and supplies.
- Coordinate processing with the Disaster Recovery Team leader.
- Notify the ROC when processing begins and ends, and if problems occur.
- Document actions.
- Return processed administrative documents to the ROC.

#### SITE RECONSTRUCTION TEAM

- Meet with the Disaster Management Team at the time/place designated.
- Develop plan to return site to operational status as soon as possible.
- Rebuild, refurbish and equip the site.
- Coordinate the move back into the site.

## **EQUIPMENT REQUIREMENTS**

The following is the minimum equipment needed to support high priority administrative applications for the period immediately after a disaster requiring recovery site processing:

- Vehicle for transportation to recovery site. NOTE: A car is immediately available - ITS university car - plus personal vehicles.
- Backup tapes of the administrative system(s) and computer system tapes to be collected from off-site location.

## **STUDENT COMPUTER CENTER (SCC) FILE SERVERS**

Student Computer Center PC and Macintoshes are served by two Novell file servers (SCC1 and SCC2).

SCC1: IBM PC Server 325; 288 MB RAM, 8.5 GB HD capacity; Novell 4.11 250 user license.

SCC2: IBM PC Server 520; 160 MB RAM, 8.5 GB HD capacity; Novell 4.11 250 user license.

The SCC file servers are configured as functional images of each other. In the event of system failure of either system, the other server can be quickly reconfigured to pick up entire load.

## **SUPPLY REQUIREMENTS**

The minimum supplies needed to support off-site processing of administrative applications are identified in Appendix I, Attachment 2, "Supplies Checklist."

## ACADEMIC SYSTEM DISABLED

### **RESPONSIBILITIES/ACTIONS**

#### SENIOR OPERATOR ON DUTY

- Notify Public Safety and Cedar Falls Fire Department, as the situation dictates.
- Notify the Systems & Operations Manager of the event and the current status.
- Verify Current Backups are locked in ITS safe.
- Perform system shutdown and other emergency procedures, and/or evacuate the facility, if necessary.

#### DEC SYSTEMS ADMINISTRATOR

- Determine the extent of the disaster to personnel, equipment, facility and operational capability.
- Notify the Associate Vice President for Information Technology of the event and current status.
- Provide data to assist the Associate Vice President for Information Technology in identifying the time and place to convene the Disaster Management Team.
- Notify the Systems & Operations Manager of the event, and to continue the alert roster and convene the Disaster Management Team.
- Notify the vendor for maintenance support.
- Identify what, if any, functions can continue on-site.
- Collect system backup tapes or retrieve from FirStar Bank.
- Assemble vital documents, or retrieve from off-site location.
- Meet with the Disaster Management Team at the time/place designated.
- Provide a schedule of operators.
- Coordinate processing priorities with the Recovery Team.

#### UNIX SYSTEMS ADMINISTRATOR

- Notify the Systems & Operations Manager to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Provide a schedule of operators.
- Identify and notify operator(s) for Recovery Team, if necessary.
- Coordinate processing priorities with the team.

#### ASSOCIATE VICE PRESIDENT FOR INFORMATION TECHNOLOGY

(Disaster Plan Coordinator)

If a minor disaster:

- Determine whether or not to assemble the Disaster Management Team (DMT).

If the DMT is to be assembled:

- Meet with the Disaster Management Team at the time/place designated.

- When the team is assembled, determine expected processing needs.
- Establish processing priorities and scheduling requirements.
- Assemble and brief the Recovery Team, as necessary.
- Document actions.

For major and catastrophic disasters, also:

- Establish a Recovery Operations Center (ROC) for coordination of all recovery activities.
- Schedule personnel to staff the ROC.
- Establish escalation/de-escalation plans.
- Assemble and brief the Site Reconstruction Team.

#### SYSTEMS & OPERATIONS MANAGER

- Notify the Information Systems Director to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Coordinate any system programming requirements.
- Provide a schedule of system programmers.
- Collect development backup tapes or retrieve from FirStar Bank or have FirStar Bank deliver to the recovery site, as applicable.
- Coordinate communications requirements.

#### INFORMATION SYSTEMS DIRECTOR

- Notify the Network Services Director to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Determine which critical applications are dependent upon data communications and what can be done (on-line systems).
- Coordinate communications requirements.
- Provide the team with a schedule of administrative programmers.
- Identify and notify programmers for Recovery Team, if necessary.
- Determine administrative development processing needs during expected down time.
- Coordinate priorities and establish a processing schedule.

#### NETWORK SERVICES DIRECTOR

- Notify the User Services Director to continue alert roster, and convene Disaster Management Team.
- Meet with the Disaster Management Team at the time/place designated.
- Determine which critical applications are dependent upon data communications and what can be done (on-line systems).
- Establish required communications.
- Coordinate communications requirements.
- Provide a schedule of communications personnel.
- Identify and notify specialist for Recovery Team.

### USER SERVICES DIRECTOR

- Meet with the Disaster Management Team at the time/place designated.
- Notify users of the level of service available.
- Provide a schedule of User Services personnel.
- Identify and notify the User Services individual who will be member of the Recovery Team.
- Determine data entry needs and coordinate requirements.
- Coordinate communication between User Services and Recovery Team.
- Provide for distribution of development documents.

### RECOVERY TEAM

- Meet with the Disaster Management Team at the time/place designated.
- Proceed to alternate site with required software, equipment, documentation, and supplies.
- Coordinate processing with the Disaster Recovery Team leader.
- Notify the ROC when processing begins and ends, and if problems occur.
- Document actions.

### SITE RECONSTRUCTION TEAM

- Meet with the Disaster Management Team at the time/place designated.
- Develop plan to return site to operational status as soon as possible.
- Rebuild, refurbish and equip the site.
- Coordinate the move back into the site.

### **EQUIPMENT REQUIREMENTS**

The following is the minimum equipment needed to support priority development applications for the period immediately after a disaster requiring alternate site processing:

- Vehicle for transportation to and from the alternate site. NOTE: One car is immediately available (ITS transportation car) - plus personal vehicles.
- Backup tapes of the information systems and computer system tapes to be run on the IBM. (NOTE: Arrangements for FirStar Bank to deliver these tapes to the alternate site may be necessary.)

The following is the equipment and software inventory of ITS mainframe systems:

Hardware/Software Environment  
August 1, 1999

ADMINISTRATIVE HARDWARE

Mainframe Computer	1	IBM 9672-R12; 12 ESCON, 9 Parallel, 2 OSA, 512mb
Console	1	IBM 3278
Disk Controller	2	IBM 3990-xxx
Disk Drives	1	IBM 3390-A28
	1	IBM 3390-B2C
	1	9391-A10 RAMAC Storage Rack
	16	9392-B23 Storage Drawers
Tape Controller	1	STC 4551 (300-6250 BPI)
Tape Drives	1	IBM 3490E-C22 (36 track)
Printers	1	IBM 6262-014 (1400 LPM)
	1	IBM 3816-016D (16 PPM)
	1	IBM 3930-02D (30 PPM)
Local Comm		
Controllers	1	IBM 3174-01L
Controllers	1	IBM 3174-01L (w/Token-Ring Support)
Printer	1	IBM 3287 Emulation on ProPrinter
Multiplexers	8	IBM 3299
Remote Comm		
9600 Baud Modems	28	Gandalf/Penril V.32/V.42/V.42bis
28.8 K-Baud Modems	60	US Robotics V.34

ADMINISTRATIVE SOFTWARE

Operating System	IBM OS/390 1.2 MVS OS/390 1.2 JES2 ACF/VTAM 4.3.0 TSO/E 2.5.0 ISPF 4.3 SDSF 1.6.0 SMP/E 1.8.1 RMF 5.2.0 EREP 3.5.0 DFP 1.3.0 DSF 1.16.0
Data Base System	Cincom Systems - Supra 2.6.10 (Relational DBMS) MANTIS 5.3 Mantis XREF Comprehensive Retrieval Utilities
Security Package	IBM - RACF 2.2 (OS/390 1.2 Security Server)
Teleprocessing Monitor	IBM - CICS/ESA 4.1.0 IBM - TCP/IP 3.1
Job Tracking	Legent/CA JobTrac 3.4
Performance Monitor	Landmark TMON MVS 2.0
Editor	IBM - ISPF 4.3.0
Sort Package	IBM DFSort 1.13.0
DASD Backup	Innovation Data Processing Fast Dump Restore (FDR/CPK) 5.3
4th Generation Languages Compilers	MANTIS 5.3 IBM - ANS COBOL 1.2.4 IBM - COBOL for MVS & VM 1.2.0 IBM - HLA 1.2.0
Utilities	IBM - 3270 PC FILE TRANSFER 1.1.1 IBM - DITTO/ESA 1.1
Print Utilities	IBM - PSF 2.02.0 IBM - PPFA 1.1.0 IBM - OGL/370 1.1
Report Writer	Sterling Software - MARK IV 10.0

ACADEMIC HARDWARE

- 1 DEC Alpha AXP 4000-610
  - 14 DEC RZ26 disk drive
  - 1 DEC RRD42 CD drive
  - 1 DEC TSZ07 tape drive
  - 1 DEC TLZ06 tape drive
  - 1 DEC LP29 line printer
- 1 DEC AlphaServer 2000 4/200
  - 4 DEC RZ28 disk drive
  - 1 DEC RRD43 CD drive
  - 1 DEC TLZ6L DAT Loader
- 1 DEC Alpha Server 4100 5/533
  - 4 4.3gb
  - 14 4.3gb in two RAID array
  - 1 TZ89 DCT tape
  - 1 TLZ7 4mm DAT tape
  - 1 H5Z70 RAID array
  - 24 9.1gb drives
- 1 DEC VAXstation 4000 VLC
  - 1 DEC VRC16 color monitor
  - 1 DEC RZ26 disk drive
  - 1 DEC RZ24L disk drive
  - 1 DEC SZ03 expansion cabinet
- 1 DEC VAXstation 3100 Model 80
  - 1 DEC VR262 monochrome monitor
  - 3 DEC RZ23 disk drive
  - 1 DEC RRD40 CD drive
  - 1 DEC TZ30 tape drive
- 1 Sun SPARCstation 10 Model 30 (iscssun.uni.edu)
  - 1 Sun X569A Disk Pack (2 X 1.05GB)
  - 1 Sun X541A Disk Drive (5.35GB)
  - 1 Sun X559A CD Drive
  - 1 Sun XTAP8MM Tape Drive
- 1 Sun ULTRA1 Model 140 (goofy.uni.edu)
  - 1 SPARCstorage MultiPak (2 X 4.5GB)
- 1 Sun ULTRA1 Model 140 (access.admin.uni.edu)
  - 1 SPARCstorage MultiPak (2 X 4.5GB)
- 1 Sun ULTRA1 Model 140 (unisql.admin.uni.edu)
- 1 Sun ULTRA1 Model 140 (news.uni.edu)
  - 1 SPARCstorage MultiPak (3 X 4.5GB)

- 1 Sun SPARCstation 4 Model 110 (dns.uni.edu)
  - 1 Sun X541A Disk Drive (4.5GB)
  
- 1 Sun ULTRA 10 (sparky.uni.edu)
  - 1 Sun X814A Tape Drive
  
- 1 Sun Enterprise250 (panther.uni.edu)
  - 1 Sun StorEDGE D1000 (6 X 9.0GB)
  - 1 Sun XTAPDL-021A Tape Drive
  - 1 Sun GDM-1962B Color Monitor
  
- 1 IBM RS/6000 43P Model 7248-132 (oldblu.admin.uni.edu)
  - 1 IBM P50 Color Monitor
  
- 1 IBM RS/6000 43P Model 7043-150 (risky.admin.uni.edu)
  - 1 IBM 7206-005 4mm Tape Drive
  - 1 IBM P92 Color Monitor

**ACADEMIC SOFTWARE**

- 3.0 DEC ADA for OpenVMS AXP
- 4.1 MU7AA DEC C for OpenVMS AXP
- 2.1 VAX COBOL for OpenVMS AXP
- 11.2 DECset for OpenVMS AXP
- 6.2 DEC FORTRAN for OpenVMS AXP
- 3.1 VAX Language Sensitive Editor
- 2.5 DEC Notes for OpenVMS AXP
- 5.2 DEC Pascal for OpenVMS AXP
- 5.5-2 OpenVMS VAX
- 6.1 OpenVMS AXP
- 5.5-2 DECnet/OSI FF OpenVMS VAX
- 6.1 DECnet/OSI End-Node OpenVMS AXP
- 5.5-2 VBRAA VAX Cluster
- 6.1 VMS Cluster Software for OpenVMS AXP
- 1.2 DSNlink for OpenVMS AXP
- 3.1 DECserver 200
- 2.0 DECserver 250
- 1.1 DECserver 700
- 4.1 SPSS
- 6.07 SAS
- 5.0.4 PMDF
- 3.4 MultiNet
- 9.1 Minitab
- DEC C++

**SUPPLY REQUIREMENTS**

The minimum supplies needed to support off-site processing of administrative applications are identified in Appendix I, Attachment 2, "Supplies Checklist."

## APPENDIX I, Attachment 1

**ITS CALL IN INFORMATION**

Loss of air conditioning and/or electricity in Curris Business Building, Gilchrist Hall, and/or Baker 13.

At any time there is a loss of air conditioning and/or electricity, use this list, in order, until one of the following persons is contacted. This is prior to and in addition to calling the on-call person for the Physical Plant.

	Office
ITS Computer Room	273-2046
Ken Connelly	273-5850
Steve Moon	273-6813
Gene Lawin	273-2947
Bob Hetrick	273-2961
Randy Maas	273-3001
Keith Young	273-2008
Doug Case	273-7145
Clyde Luck	273-2289
Dave Kacmarynski	273-2046
Jimmy Mixdorf	273-2046
Denise Patterson	273-2046
Garry Bozylinsky	273-7779

Problems with any of the ITS Student Computer Centers (Curris Business, Library, Maucker, Redeker, Schindler and Towers) should be directed to the following individuals in order:

	Office
Scott Hunt	273-6981
Consulting Center	273-5555
Amanda Schima	273-6981
Robert Meier	273-6981
Diane Sullivan	273-6814
Tom Peterson	273-6460
Steve Moon	273-6813
Garry Bozylinsky	273-7779

For urgent problems that occur during normal business hours, contact the office.

For non-urgent problems, please e-mail [US-SCCSUPPORT@uni.edu](mailto:US-SCCSUPPORT@uni.edu) with a description of the problem.

**EMERGENCY ALERT ROSTER**

Ken Connelly	Systems & Operations Manager	35850
Dennis Lindner	Information Systems Director	32424
Steve Moon	Network Services Director	36813
Tom Peterson	User Services Director	36460
Garry Bozylinsky	Associate Vice President for IT	37779

**BACKUP ALERT ROSTER**

Kevan Forest	Data Base Admin	32453
Randy Maas	Senior Systems Programmer	33001
Gene Lawin	Computer Network Systems Manager	32947
Jack Miller	Consulting Center Coordinator	35943
Kevin Quarnstrom	Information Systems Manager	32444
Diane Sullivan	Support Services Manager	36814
Randy Hayes	Voice Services Manager	37473
Keith Young	Systems Programmer	32008

**NETWORK ACTION TEAMS**

In the event of a reported failure with one of the many different "Network" attached devices on campus, the following hardware/application/system software teams should be contacted.

Care must be taken in evaluating the severity of the "Network" problem, before contacting the individuals directly. Instances of a single networked station not communicating properly may be an emergency to the user, but may not warrant pulling staff off task to troubleshoot.

Isolated problems should be reported in the normal fashion through the Consulting Center ESR/Software reporting schemes or by contacting the Systems and Operations staff at 36822. In the event of multiple stations or hosts not functioning properly in the networked environment, contact all members of the appropriate network action team.

If you cannot contact members of the team directly, report the problems to the appropriate unit manager.

**Contacts:**

Gene Lawin	Ken Connelly	Jolene Griffin	Steve Moon
Doug Case	Diane Sullivan	Barb Mardis	Jon Wolter
Ken Bauer	Julie Heiple	Brett S	Aaron Morgan
Mike Savage	Steve Larson	Tom Turner	Mark Renner

	<u>Primary Contact</u>	<u>Backup Contact</u>
Local Area Networks - Novell Network		
a)	Student Labs	
	Appl : Diane S.(36814)	Doug C.(37145)
	OS System: Doug C.(37145)	Gene L.(32947)
	Hardware: Jon W.(36834)	Aaron M.(32871)
b)	ITS and VPAF	
	Appl: Diane S.(36814)	Doug C.(37145)
	OS System: Doug C.(37145)	Gene L.(32947)
	Hardware: Jon W.(36834)	Aaron M.(32871)
c)	CBA	
	Appl: Brett S.(33062)	Barb M.(32402)
	OS System: Brett S.(33062)	Doug C.(37145)
	Hardware: Jon W.(36834)	Aaron M.(32871)
d)	Northern Iowan	
	Appl: Diane S.(36814)	Doug C.(37145)
	OS System: Doug C.(37145)	Gene L.(32947)
	Hardware: Jon W.(36834)	Aaron M.(32871)
e)	Continuing Education	
	Appl: Mike S.(37885)	Diane S.(36814)
	OS System: Mike S.(37885)	Doug C.(37145)
	Hardware: Aaron M.(32871)	Jon W.(36834)
f)	CHFA	
	Appl: Steve L.(36314)	Doug C.(37145)
	OS System: Doug C.(37145)	Steve L.(36314)
	Hardware: Jon W.(36834)	Aaron M.(32871)
g)	CSBS	
	Appl: Tom T.(33112)	
	OS System: Tom T.(33112)	Doug C.(37145)
	Hardware: Jon W.(36834)	Aaron M.(32871)
h)	CSBR	
	Appl: Tom T.(33112)	
	OS System: Doug C.(37145)	Gene L.(32947)
	Hardware: Jon W.(36834)	Aaron M.(32871)

- i) WebFocus  
 Appl: Julie H.(37431) Gene L.(32947)  
 OS System: Gene L.(32947)  
 Hardware: Jon W.(36834) Aaron M.(32871)
- j) CD-ROM  
 Appl: Ken B.(36256) Gene L.(32947)  
 OS System: Ken B.(36256) Doug C.(37145)  
 Hardware: Jon W. (36834) Aaron M.(32871)
- k) ESS1  
 Appl : Diane S.(36814) Doug C.(37145)  
 OS System: Doug C.(37145) Gene L.(32947)  
 Hardware: Jon W.(36834) Aaron M.(32871)
- l) ESS2  
 Appl : Mark R.(32281) Diane S. (36814)  
 OS System: Doug C.(37145) Gene L.(32947)  
 Hardware: Jon W.(36834) Aaron M.(32871)
- Internet - (3Telnet, FTP, TCP/IP, off-campus Email  
 Software: Ken C.(35850) Steve M.(36813)  
 Hardware: Ken C.(35850) Steve M.(36813)

## APPENDIX I, Attachment 2

**SUPPLIES CHECKLIST**

This list may be modified as the particular circumstance dictate. These supplies are available at the Center. Should the Center be destroyed, a backup source must be procured. The suggested quantity is just that; the actual needs relative to the particular situation will be determined by the Disaster Management Team, with ongoing needs identified by the Disaster Recovery Team.

For cases where purchase of supplies becomes necessary, vendor information is listed on the following pages. All purchases will be handled through normal Purchasing procedures, but with an emergency priority.

ITEM	SUGGESTED QUANTITY	ACTUAL NEEDS
___ Scratch Tapes	50	_____
___ Production Documentation (Set)	1	_____
___ Paper (Boxes)1-Part	10	_____
___       2-Part	5	_____
___       3-Part	5	_____
___       4-Part	5	_____
Special Forms (Boxes)		
___       PAFs	5	_____
___       644E	3	_____
___       644F	3	_____
___       AP Checks	2	_____
___       Payroll Checks (Number)	4,000	_____
___ Forms List	1	_____
___ Printer Ribbons	10	_____
___ Boxes for Output	5	_____
___ Operator Manuals	1	_____
___ Scratch Paper/Pencils/Pens	As Needed	As Needed

## APPENDIX I, Attachment 3

**COMPUTER PRINT FORMS INFORMATION**

#	Description	Req #	PO #	Vendor	Qty	Unit Price
1001	VAX LP29 LINE RIBBONS	S6034	H05193	Lefler Limited	10	\$15.67
1011	PRINTRONIX P-300 RIBBONS	L4015	A02190	Data Source Media	6	\$3.99
1015	SCANNER RIBBONS	T6022	VISA	Staples	10	\$6.00
1060	APPLE IMG WRT 2 RIBBONS	M1060	B01508	Lefler Limited	42	\$1.46
1073	PANASONIC KX-P1180 RIBBON	S6033	H04344	Media Recovery	21	\$2.45
1074	PANASONIC KXP-2180 RIBBON	S6038	H05502	Media Recovery	132	\$3.51
1083	H-P LASERJET CARTRIDGE	S6033	H04344	Media Recovery	5	\$60.49
1084	H-P DESK JET 500 CARTRIDGE	VISA	VISA	Cedar Computer	7	\$25.31
1085	IBM HIGH YIELD CARTRIDGE	S6011	H02142	Media Recovery	1	\$169.99
1085	IBM HIGH YIELD CARTRIDGE	S6011	H02142	Media Recovery	2	\$172.15
1087	HP DESKJET COLOR CARTRIDGE	T6012	VISA	Cedar Computer	3	\$26.00
1088	HP4MV TONER CARTRIDGE	Z6003	M01008	Media Recovery	47	\$111.80
1089	HP 6P TONER CARTRIDGE	W6037A	K03238	Data Source Media	17	\$74.00
1090	STK 1500 PRINTER RIBBONS	W6023	K02153	Media Recovery	3	\$14.89
1090	STK 1500 PRINTER RIBBONS	W6023	K02153	Media Recovery	18	\$14.10
1091	IBM 6262 PRINTER RIBBONS	W6046	K04965	Data Source Media	28	\$13.50
1092	CANON BJC-210 COLOR CART.	W6010	K00948	CompUCom Systems	3	\$34.34
1098	IBM HP 8100 LASER CARTRIDGE	Z6004	M01007	Media Recovery	175	\$153.34
1719	PHOTOCONDUCTOR IBM 3816	W6027	K02297	Media Recovery	1	\$358.52
1720	DEVELOPER UNIT IBM 3816	S6043	82563	Campus Supply	1	\$937.50
1720	DEVELOPER UNIT IBM 3816	S6043	82563	Campus Supply	2	\$823.37
1725	CLEANING UNIT IBM 3816	W6009	K00962	Data Source Media	3	\$369.00
1726	LASER CARTRIDGE IBM 3816	W6008	K00963	Data Source Media	2	\$49.98
1752	FUSER UNIT IBM 3816	W6041	K03696	Iowa Business Machines	1	\$622.78
1752	FUSER UNIT IBM 3816	W6041	K03696	Iowa Business Machines	2	\$680.00
1840	3930 TONER CARTRIDGE	T6044	J04330	Media Recovery	12	\$31.53
1841	3930 DEVELOPER UNIT	T6023	J02047	Iowa Business Machines	3	\$527.17
1842	3930 CLEANING UNIT	T6027	J02859	Data Source Media	8	\$319.50
1843	3930 PHOTOCONDUCTOR UNIT	W6033	K03041	Data Source Media	6	\$302.00
1845	3930 FUSER UNIT	W6036	K03245	Data Source Media	5	\$630.00

1900	IBM 3490-C22 CLEANING CART.	VISA	VISA	Iowa Business Machines	1	\$19.95
1900	IBM 3490-C22 CLEANING CART.	VISA	VISA	Iowa Business Machines	1	\$17.00
3004	8mm DIGITAL TAPES	W6017	K01704	Data Source Media	67	\$10.11
3005	4mm DAT TAPES	W6034	K03032	Comp USA Direct	16	\$8.99
3006	DAT CLEANING TAPES	S6047	H06700	DEC Direct	1	\$12.35
3006	DAT CLEANING TAPES	S6047	H06700	DEC Direct	7	\$12.37
3007	COMPAQ TAPEIV Data Cartridge	T6042	J04238	Cedar Computer	11	\$80.00
5001	3.5 x 15/16 LABEL 1 UP	W6013	K01467	OEI	90,000	\$2.06
5001	3.5 x 15/16 LABEL 1 UP	W6013	K01467	OEI	500,000	\$1.99
5002	3.5 X 16/16 LABEL 3 UP	M04003	B01509	Data Documents	45,000	\$1.67
5006	5 X 15/16 LABEL	T6014	J01318	Data Documents	5,000	\$5.49
5006	5 X 15/16 LABEL	T6014	J01318	Data Documents	5,000	\$4.11
5008	3.5 X 7/16 LABELS	W6029	K02330	Corporate Express	90,000	\$1.20
5181	11.75 X 8.5 - 1 PART	W6028	K02329	OEI	45,500	\$6.70
5182	11.75 X 8.5 - 2 PART	T6038	J03333	OEI	15,000	\$20.04
5183	11.75 X 8.5 - 3 PART	T6032	J03064	OEI	3,000	\$32.04
5411	14 7/8 X 11 - 1 PART	T6010	J01303	OEI	8,940	\$51.43
5412	14 7/8 X 11 - 2 PART	T6029	J02868	OEI	24,000	\$20.59
5413	14 7/8 X 11 - 3 PART	W6016	K01291	OEI	7,000	\$35.27
5481	14 7/8 X 8 1/2", 15#, 1 PLY, GRNB	W6004	K01273	Waterloo Paper	91,000	\$5.70
5811	8.5 X 11 - 1 PART	W6039	K03342	OEI	91,000	\$5.79
5831	8.5 X 3.5 - 1 PART UNLINED	W6014	K01166	OEI	16,500	\$3.43
5851	8.5 X 5.5 - 1 PART UNLINED 20#	W6042	K03741	Waterloo Paper	70,200	\$3.49
5910	9.5 X 11 - 1 PART UNL 20#	P4059	E10228	OEI	35,000	\$8.88
5913	9.5 X 11 - 3 PART	M4015	88661	UNI Print Services	1,000	\$23.30
7109	14 7/8 X 11 - 1 PT UNRULED	L4063	A11021	OEI	2,600	\$17.88
8001	8.5 X 11 - 20# XEROX COPY	Z6001	M00858	OEI	45,000	\$4.10
8002	8.5 X 14 - 20# XEROX COPY	M4068	84259	Campus Supply	1,000	\$5.46
8006	STUDENT ASSESMENT ENV.	W6019	80922030	UNI Print Services	3,500	\$97.40
8007	ORAL COMPETENCE FORM	T6034	J03093	NCS Forms Division	22,500	\$73.42
8008	STUDENT ASSESSMENTS	W6047	K05133	NCS Forms Division	12,500	\$54.10
8008	STUDENT ASSESSMENT	W6047	K05133	NCS Forms Division	75,000	\$56.03
2600	Merit Time Sheets	W6048	K05310	NCS Forms Division	12,500	\$62.49
6401	Certificate of Enrollment Form	W6018	K01733	Script Safe Security Prod.	6,000	\$15.07
6411	D & F Letters	T6017	J01378	HDC	13,400	\$105.90
6414	Internal Transcripts	W6044	K04364	American Business Forms	41,600	\$12.48

6416	External Transcripts	W6020	K01829	Script Safe Security Prod.	33,000	\$44.86
6550	UNI ID Cards	T6015	J01289	Data Documents	12,800	\$26.84
6601	Fixed Asset Inventory	W6022	K02089	Corporate Express	7,150	\$57.61
6602	Fixed Quotations	R4047	G10359	American Business Forms	1,800	\$118.47
6606	Deposit Slips	S6002	H02250	American Business Forms	1,800	\$13.09
6621	Accounts Receivable Statement	W6037B	K03309	OEI	134,500	\$12.69
6628	3 Part - 3 ply Voucher with Carbons	W6038	K03290	HDC	28,920	\$46.05
6629	Purchase Order Form	T6007	J01299	Rapid Business Systems	8,100	\$65.94
6630	Financial Aid Award Letter	W6031	K02872	American Business Forms	2,400	\$48.15
6631	Financial Aid Award Letter	R4033	G06179	American Business Forms	13,000	\$48.15
6640	Financial Aid Labels 7 1/2 x 1 3/4	L4028	A05076	Rapid Business Systems	17,500	\$40.46
6650	Perkins Loan Truth in Lending State.	W6001	K00728	Rapid Business Systems	3,300	\$130.94
6651	Perkins Loan Promissory Note w/pnk	S6048	H07667	OEI	1,100	\$152.29
6653	Perkins Loan Promissory Note	W6002	K00760	OEI	1,800	\$140.80
6660	Stafford Promissory Note			US Government	4,000	\$-
6661	Direct Plus Loan Promissory Note			US Government	4,500	\$-
6670	Direct Stafford Promissory Notes			US Government	5,500	\$-
6671	Direct Master Promissory Note			US Government	18,000	\$-
6701	Physical Plant Job Cards	W6026	K02451	Matt Parrott	74,800	\$8.98
6803	Phone Campaign Card # 1	T6013	J01368	HDC	4,000	\$13.88
6805	Foundation Reminder Letters	P4056	5041438	UNI Print Services	16,000	\$17.83

**VENDORS**

American Business Forms  
Rod Johnson  
PO Box 1415  
Minneapolis, MN 55480-1415  
800-529-1980  
(319)882-4214

Cedar Computer  
Deb Grubich  
2345 Blairsferry Road NE  
Cedar Rapids, IA 52402  
800-597-0555  
(319)393-7362

Comp USA Direct  
Rod Vozella  
34 St. Martin Drive  
Marlboro, MA 1752  
800-669-4727

CompUCom Systems, Inc.  
Deb Grubich  
2345 Blairsferry Road NE  
Cedar Rapids, IA 52402  
800-597-0555  
(319)393-7362

Corporate Express  
101 2<sup>nd</sup> Street SE  
Cedar Rapids, IA 52401  
800-397-8309

Data Documents  
101 2<sup>nd</sup> Street SE  
Cedar Rapids, IA 52401  
800-397-8309

Data Source Media  
Pam Johnson  
PO Box 4397  
Lincoln, NE 68504  
800-737-7075  
(402)466-3342

DEC Direct  
PO Box CS2008  
Nashua, NH 03061-2008  
800-344-4825

HDC  
Marcia  
PO Box 2455  
Cedar Rapids, IA 52406  
(319)393-3488

Iowa Business Machines  
Mona  
614 Lafayette  
Waterloo, IA 50703  
(319)235-0346

Lefler Limited  
PO Box 503014  
St. Louis, MO 63150-3014  
(314)432-3066

Matt Parrot  
PO Box 660  
Waterloo, IA 50704-0660  
(319)234-4621

Media Recovery  
Carolyn Leutwyler  
917 State St.  
Bettendorf, IA 52722  
(319)359-5353

Morris Printing  
Steve Morris  
PO Box 1101  
Waterloo, IA 50701  
(319)234-2883

NCS Forms Division  
Patty Meier  
2125 4<sup>th</sup> St. N.W.  
Owatanna, MN 55060  
800-533-0518  
(507)455-4150

OEI  
Andrea Helbling  
4377 NW 112<sup>th</sup> St.  
Urbandale, IA 50322-2073  
800-886-4291  
(515)276-1634

Rapid Business Systems  
Connie Morningstar  
285 33<sup>rd</sup> Ave. SW  
Cedar Rapids, IA 52404  
(319)363-8817

Scrip Safe Security Products  
Linda  
11319 Grooms Road  
Cincinnati OH 45242  
800-736-7319

Staples  
1542 Flammang Drive  
Waterloo, IA 50702  
(319)232-3700

Campus Supply  
Cedar Falls, IA 50614  
(319)273-2451

Print Services  
Cedar Falls, IA 50614  
(319)273-2448

US Government  
Dept. of Education  
800-848-0978

Waterloo Paper  
Bob Harrison  
200 Sycamore St.  
Waterloo, IA 50703  
800-595-3596  
(319)234-4459

APPENDIX I, Attachment 4

**ADMINISTRATIVE SYSTEM BACKUP PROCEDURES**

The following document is maintain as an electronic file documentation of the administrative systems.

```

*****
UNIVERSITY OF NORTHERN IOWA    BACKUP PROCEDURES
*****

```

The following backup procedures have been established for disaster recovery and for other unforeseen problems that would require restoring the data files maintained on the central administrative computer. Innovation Data Processing's Fast Dump Restore (FDR) is used to backup disk files and/or entire disk volumes onto magnetic tape so that this data can be stored in a secure location, which in some cases is off sight.

Information about each of the scheduled backup procedures follows:

- ```

*****
*      FIVE O'CLOCK BACKUPS - DATABASE FILES      *
*      NIGHTLY BACKUPS - ALL DASD                  *
*      WEEKLY BACKUPS (TUESDAY) ALL DASD          *
*      MONTHLY BACKUPS (10TH WORKING DAY) ALL DASD *
*      MONTHLY BACKUPS - SOURCE CODE              *
*      SEMESTERLY BACKUPS - STUDENT INFORMATION    *
*****

```

```
*****  
**  
** FIVE O'CLOCK BACKUPS - DATABASE FILES **  
**  
*****
```

SCHEDULE: Daily, immediately after the on-line system is brought down.  
(normally 5:30 p.m.)

CONTENTS: All Production Database Files.

GENERATIONS: One. (Retained for minimum of 24 hours)

STORED: Fireproof vault in Computer Room.

DATASET NAMES: X11109.VOCLOCK.C.DB0001  
X11109.VOCLOCK.C.DB0002  
X11109.VOCLOCK.C.DB0003  
X11109.VOCLOCK.C.DB0004  
X11109.VOCLOCK.C.DB0005  
X11109.VOCLOCK.C.DB0006  
X11109.VOCLOCK.C.DB0007  
X11109.VOCLOCK.C.DB0008

```
*****  
**  
** NIGHTLY BACKUPS - ALL DASD **  
**  
*****
```

SCHEDULE: Daily, last thing each night after all production batch jobs have been processed (normally around midnight).

CONTENTS: All DASD.

GENERATIONS: Five.

STORED: Fireproof vault in Computer Room until next backup is made; then to tape racks in Computer Room.

DATASET NAMES: X11109.NIGHTLY.DB0001 X11109.NIGHTLY.HIST01  
X11109.NIGHTLY.DB0002 X11109.NIGHTLY.HIST02  
X11109.NIGHTLY.DB0003 X11109.NIGHTLY.WK0001  
X11109.NIGHTLY.DB0004 X11109.NIGHTLY.WK0002  
X11109.NIGHTLY.DB0005 X11109.NIGHTLY.WK0003  
X11109.NIGHTLY.DB0006 X11109.NIGHTLY.WK0004  
X11109.NIGHTLY.DB0007 X11109.NIGHTLY.WK0005  
X11109.NIGHTLY.DB0008 X11109.NIGHTLY.WK0006  
X11109.NIGHTLY.LIB001 X11109.NIGHTLY.WK0007  
X11109.NIGHTLY.LIB222 X11109.NIGHTLY.WK0008  
X11109.NIGHTLY.LIB333 X11109.NIGHTLY.WK0009  
X11109.NIGHTLY.LIB444 X11109.NIGHTLY.WK0010  
X11109.NIGHTLY.ITSRES X11109.NIGHTLY.WK0011  
X11109.NIGHTLY.ITSDL1  
X11109.NIGHTLY.ITSSMP  
X11109.NIGHTLY.CIC111  
X11109.NIGHTLY.IOD111  
X11109.NIGHTLY.RAC111  
X11109.NIGHTLY.ITSDL2  
X11109.NIGHTLY.SPL777  
X11109.NIGHTLY.ARC000  
X11109.NIGHTLY.ARC111  
X11109.NIGHTLY.CAT111  
X11109.NIGHTLY.CAT222  
X11109.NIGHTLY.ITSCAT  
X11109.NIGHTLY.TSO001  
X11109.NIGHTLY.TSO002  
X11109.NIGHTLY.TSTPK1  
X11109.NIGHTLY.TSTPK2

```
*****  
**  
** WEEKLY BACKUPS (TUESDAY) - ALL DASD **  
**  
*****
```

SCHEDULE: Weekly, last thing at night after all production batch jobs have been processed on Tuesday

CONTENTS: All DASD.

GENERATIONS: Three

STORED: FirStar Bank vault until next backup is made;  
then to tape racks in Computer Room.

DATASET NAMES: X11109.WEEKLY.DB0001 X11109.WEEKLY.HIST01  
X11109.WEEKLY.DB0002 X11109.WEEKLY.HIST02  
X11109.WEEKLY.DB0003 X11109.WEEKLY.WK0001  
X11109.WEEKLY.DB0004 X11109.WEEKLY.WK0002  
X11109.WEEKLY.DB0005 X11109.WEEKLY.WK0003  
X11109.WEEKLY.DB0006 X11109.WEEKLY.WK0004  
X11109.WEEKLY.DB0007 X11109.WEEKLY.WK0005  
X11109.WEEKLY.DB0008 X11109.WEEKLY.WK0006  
X11109.WEEKLY.LIB001 X11109.WEEKLY.WK0007  
X11109.WEEKLY.LIB222 X11109.WEEKLY.WK0008  
X11109.WEEKLY.LIB333 X11109.WEEKLY.WK0009  
X11109.WEEKLY.LIB444 X11109.WEEKLY.WK0010  
X11109.WEEKLY.ITSRES X11109.WEEKLY.WK0011  
X11109.WEEKLY.ITSDL1  
X11109.WEEKLY.ITSSMP  
X11109.WEEKLY.CIC111  
X11109.WEEKLY.IOD111  
X11109.WEEKLY.RAC111  
X11109.WEEKLY.ITSDL2  
X11109.WEEKLY.SPL777  
X11109.WEEKLY.ARC000  
X11109.WEEKLY.ARC111  
X11109.WEEKLY.CAT111  
X11109.WEEKLY.CAT222  
X11109.WEEKLY.ITSCAT  
X11109.WEEKLY.TSO001  
X11109.WEEKLY.TSO002  
X11109.WEEKLY.TSTPK1  
X11109.WEEKLY.TSTPK2

```
*****
**
**   MONTHLY BACKUPS (10th WORKING DAY) - ALL DASD   **
**
*****
```

SCHEDULE: Monthly, last thing at night after all production batch jobs have been processed (normally on the 10<sup>th</sup> working day of each month)

CONTENTS: All DASD.

GENERATIONS: Three

STORED: FirStar Bank vault until next backup is made; then to tape racks in Computer Room.

DATASET NAMES: X11109.MONTHLY.DB0001 X11109.MONTHLY.HIST01  
X11109.MONTHLY.DB0002 X11109.MONTHLY.HIST02  
X11109.MONTHLY.DB0003 X11109.MONTHLY.WK0001  
X11109.MONTHLY.DB0004 X11109.MONTHLY.WK0002  
X11109.MONTHLY.DB0005 X11109.MONTHLY.WK0003  
X11109.MONTHLY.DB0006 X11109.MONTHLY.WK0004  
X11109.MONTHLY.DB0007 X11109.MONTHLY.WK0005  
X11109.MONTHLY.DB0008 X11109.MONTHLY.WK0006  
X11109.MONTHLY.LIB001 X11109.MONTHLY.WK0007  
X11109.MONTHLY.LIB222 X11109.MONTHLY.WK0008  
X11109.MONTHLY.LIB333 X11109.MONTHLY.WK0009  
X11109.MONTHLY.LIB444 X11109.MONTHLY.WK0010  
X11109.MONTHLY.ITSRES X11109.MONTHLY.WK0011  
X11109.MONTHLY.ITSDL1  
X11109.MONTHLY.ITSSMP  
X11109.MONTHLY.CIC111  
X11109.MONTHLY.IOD111  
X11109.MONTHLY.RAC111  
X11109.MONTHLY.ITSDL2  
X11109.MONTHLY.SPL777  
X11109.MONTHLY.ARC000  
X11109.MONTHLY.ARC111  
X11109.MONTHLY.CAT111  
X11109.MONTHLY.CAT222  
X11109.MONTHLY.ITSCAT  
X11109.MONTHLY.TSO001  
X11109.MONTHLY.TSO002  
X11109.MONTHLY.TSTPK1  
X11109.MONTHLY.TSTPK2

```
*****
**
**      MONTHLY BACKUPS - SOURCE CODE      **
**
*****
```

SCHEDULE: Monthly (normally on the 10<sup>th</sup> working day).

CONTENTS: Selected Program Source Files, Job Control Files.

GENERATIONS: Thirteen.

STORED: Most recent twelve backups at FirStar Bank.  
 Oldest backup in Computer Room.

DATASET NAME: X11109.SOURCE.BACKUP

The following source data is backed up:

|                           |                                                 |
|---------------------------|-------------------------------------------------|
| LMSII.SL1                 | COBOL programs source code                      |
| LMSII.SL2                 | COBOL programs source code                      |
| UNI.MARKIV.PGMS           | MARKIV program code                             |
| UNI.SCREEN.MAPS           | Screen Maps for COBOLXT Programs                |
| UNI.FIRSTRUN.CNTL         | Firstrun Library for Prod Procedures            |
| UNI.JOB.CNTL              | Production JCL Library                          |
| UNI.DB.MISC               | Database Utilities                              |
| UNI.UTIL.CNTL             | Systems Utilities                               |
| UNI.CR.PGMS               | Comprehensive Retrieval Programs                |
| UNIMVS.PROCLIB            | Production Procedure Library                    |
| UNIMVS.PRCLIB             | Test Procedure Library                          |
| UNI.PROCDOC.TEXT          | Production Procedure Documentation              |
| UNI.PROGDOC.TEXT          | Production Program Documentation                |
| UNI.DOCS.TEXT             | On-line transaction Documentation               |
| UNIMVS.SYSTEMS.MISC       | Systems Programming Utilities                   |
| UNI.COPY.LIB              | Copybook Library                                |
| UNI.FIRSTRUN.TEXT         | Firstrun Library for Prog/Proc<br>Documentation |
| X11119.PROD.LV00          | Spectra Files                                   |
| X11119.PROD.C\$IN         | Database Directory File                         |
| X11119.PROD.C\$IS         | Database Directory File                         |
| X11119.PROD.C\$IT         | Database Directory File                         |
| X11119.PROD.C\$I#         | Database Directory File                         |
| X11119.PROD.C\$ID         | Database Directory File                         |
| VSUPCICS.MANTIS.TEST.BASE | Mantis Pgm/Screen Code - Test                   |
| VSUPCICS.MANTIS.PROD.BASE | Mantis Pgm/Screen Code - Prod                   |

```

*****
**
**      SEMESTERLY BACKUPS - STUDENT INFORMATION      **
**
*****

```

SCHEDULE: Semesterly (normally September and February)

CONTENTS: All database files associated with the student records system, including the database directory. Program source code for those programs used to produce transcripts and degree audits and a narrative file explaining the contents of the backup file.

GENERATIONS: One.

STORED: University of Iowa in Iowa City.

|               |                          |                     |
|---------------|--------------------------|---------------------|
| DATASET NAME: | PRODUPSI.DB0001          |                     |
|               | PRODUPSI.DB0002          |                     |
|               | PRODUPSI.DB0003          | SI DATABASE FILES   |
|               | PRODUPSI.DB0004          |                     |
|               | PRODUPSI.DB0005          |                     |
|               | PRODUPSI.DB0006          |                     |
|               | PRODUPSI.DB0007          |                     |
|               | BACKUP.PROD.DIR.DB0001   |                     |
|               | BACKUP.PROD.DIR.DB0002   | DATABASE DIRECTORY  |
|               | BACKUP.PROD.DIR.DB0003   |                     |
|               | BACKUP.PROD.DIR.DB0004   |                     |
|               | SIS.BACKUP.PGMS.C0045070 |                     |
|               | SIS.BACKUP.PGMS.C0047041 |                     |
|               | SIS.BACKUP.PGMS.C0047042 | PROGRAM SOURCE CODE |
|               | SIS.BACKUP.PGMS.C0047080 |                     |
|               | SIS.BACKUP.PGMS.C0048044 |                     |

## APPENDIX II

### USER REACTION PLANS

#### GENERAL

Administrative User Reaction Plans are designed to provide specific guidelines for the actions to be taken by user groups (payroll, accounts payable, SIS, personnel, etc.) when the computer system is down for an extended period ("What do we do?"). Issues which must be considered are: What services will be available to you? What are your procedures for manual processing? How will you get data to the Recovery Operations Center for off-site processing? What will you do if your site is destroyed? And other specifics identified in the skeleton outline, below.

Critical operations and the time frames in which they become critical must be defined and a User Reaction Plan established for each critical business function. These plans must be independent of the master Disaster Recovery Plan, but be directly coordinated with the master plan so all involved are

fully aware of the needs and what must be done to meet those needs. Current rerun documentation may be helpful in defining specific requirements. Differences, if any, between procedures to follow for a MINOR DISASTER versus a MAJOR, or even a CATASTROPHIC DISASTER must be noted. These types of disasters are defined on page 2 (attached) of the master Disaster Recovery Plan. In some cases, it is expected that separate "scripts" or checklists should be made for each category of disaster, and a reaction (UREACT) posture identified for each. An outline of required data follows:

\_\_\_\_\_ DEPARTMENT  
USER REACTION PLAN

**GENERAL** (Basic information and concepts considered in the plan)

**RISK REDUCTION** (What you have done or need to do to reduce the potential for a disaster)

**BACKUP PROCEDURES** (Processing procedures, and off-site storage for vital documents and critical data files)

**EMERGENCY OPERATION (UREACT) PLAN**

- 1) Establish a liaison person for contact with the Recovery Operations Center.
- 2) Document the data flow of critical applications for both computer and manual processing.
- 3) Define the critical operations and the critical time frames for them.
- 4) Identify vital documents and critical data files. Provide an inventory list.
- 5) Determine an off-site storage location for these documents and data files.
- 6) Develop procedures for recovery of vital documents and data files from off-site storage location.
- 7) Determine if an off-site office location is needed.
- 8) Develop a recovery checklist for each critical function.
  - a) Determine the level of service available when notified to implement your Reaction Plan.
  - b) Establish a contact point with the Recovery Operations Center.
  - c) Establish a departmental disaster alert recall roster.
  - d) Establish a means of recovering vital records and data files.
  - e) Establish manual processing plan.
  - f) Determine telecommunication needs and backup procedures if no telecommunication is available.
  - g) Determine personnel requirements.
  - h) Determine equipment needs, and a backup source. (Do you rely on a computer system other than Information Technology Services?)
  - i) Establish a training plan.

## APPENDIX III

**MEMORANDUM OF UNDERSTANDING ALTERNATE SITE PROCESSING  
AGREEMENT AMONG THE UNIVERSITY OF NORTHERN IOWA, IOWA STATE  
UNIVERSITY, AND THE UNIVERSITY OF IOWA  
May 5, 1999**

**Purpose:** To provide administrative computing activities at the University of Northern Iowa, Iowa State University, and the University of Iowa with a backup service capability in the event of an emergency at any location. This is a reciprocal agreement.

**Scope:** This agreement pertains to each site's administrative computing services, only when an emergency condition arises at one of the participating site. Since most, if not all, computing at the host site must continue, this agreement is limited in that the sphere of services available to the guest will be governed to a great extent by the priorities of processing requirements at the time of the guest's emergency, and the time frame processing must be completed.

**General:** For the purpose of this agreement, an emergency is defined as any time when specified systems cannot be supported for various abnormal reasons. The determination of an emergency will be left to the individual parties of the agreement. The respective computer center directors at each site and/or their designated representatives, such as operations supervisors, are the personnel authorized to invoke this agreement in an emergency.

This agreement is effective upon signing by all parties and effective continuously unless revoked or amended. It will be reviewed for currency when either party determines such a need. Any part of the agreement may be amended, as dictated by the requirements of any site, upon written notification and concurrence of the directors. This agreement may be revoked after a 60-day period by written notification by any site director.

Materials and supplies will be provided by the site requiring the emergency processing. Materials supplied by the host, if any, will be replaced in kind by the user. Pre-positioning of materials is not required.

**Responsibilities:**

The site that is providing computing support (host) will:

1. Schedule available resources according to priorities established below and information provided by the supported site when this agreement is implemented.
2. Provide experienced staff as required to assist supported personnel in their service requirements.
3. Provide secure storage for materials when extended (more than one day) support is required.

The site that is receiving computing support (guest) will:

1. Notify the host site's director or representative that an emergency requirement exists, the approximate support time required, and site resources required.

2. Provide the names of the personnel who will be coming, who will be in charge of all guest activities and the approximate arrival time.
3. Make all arrangements for the transportation of personnel, programs, data, supplies, etc.

**Priorities:** Implementation details and any revised priorities applicable to a specific emergency situation will be resolved by mutual agreement of each site at the time of the emergency.

**Certification:** On behalf of their respective service units, the undersigned agree to and will comply with the provisions of this agreement.

\_\_\_\_\_  
*signature on file*  
Garry Bozylinsky, Assoc. Vice President  
Information Technology Services  
University of Northern Iowa  
255 Gilchrist Hall  
Cedar Falls, IA 50614-0007  
(319) 273-7779  
[garry.bozylinsky@uni.edu](mailto:garry.bozylinsky@uni.edu)

\_\_\_\_\_  
6/21/99  
Date

\_\_\_\_\_  
*signature on file*  
Wayne Ostendorf, Director  
Administrative Data Processing Center  
Iowa State University  
117 Pearson Hall  
Ames, IA 50011-3601  
(515) 294-2126  
[woosten@iastate.edu](mailto:woosten@iastate.edu)

\_\_\_\_\_  
6/07/99  
Date

\_\_\_\_\_  
David Dobbins, Assoc. Director  
Information Technology Services  
University of Iowa  
429 Northwestern Bell Building  
Iowa City, IA 52242  
(319) 384-0750  
[david-dobbins@uiowa.edu](mailto:david-dobbins@uiowa.edu)

\_\_\_\_\_  
Date

APPENDIX IV

**SUGGESTED LETTER TO DEPARTMENTS**

The following letter directs the establishment of User Reaction Plans (UREACT) for internal use and inclusion in the campus Administrative Systems Disaster Reaction Plan.

TO: All Offices

FROM: Garry Bozylinsky  
ITS Disaster Recovery Plan Coordinator

RE: Administrative Systems Disaster Recovery User Reaction Plans

The attached Appendix to the Administrative Disaster Recovery Plan (DRP) is provided for your guidance in developing your department's User Reaction (UREACT) Plan for emergency operation during a disaster in which the administrative computer system is down for an extended period of time. Also included are the first two pages of the DRP, which provides the plan concept and definitions used in describing levels of disaster.

Your plan, which should be completed by June 30, 1999, is to be maintained by the department. Copies should be sent to Information Technology Services for inclusion in the DRP, and to the Operations Auditor, which will review the plan for completeness. The section on backup and off-site storage of vital documents and data files is of particular note. Your plan should be tested within six months of implementation, and at least once each two years thereafter, generally in connection with a test of the entire DRP.

Please advise me when the plan is completed, when copies have been forwarded to Information Technology Services and Operations Auditor, and when the initial testing has been completed.

Attachments:

Appendix II of Disaster Recovery Plan  
First three pages of Disaster Recovery Plan

c: Operations Auditor

## APPENDIX IV

**USER REACTION PLANS****GENERAL**

Administrative User Reaction Plans are designed to provide specific guidelines for the actions to be taken by user groups (payroll, accounts payable, SIS, personnel, etc.) when the computer system is down for an extended period ("What do we do?"). Issues which must be considered are: What services will be available to you? What are your procedures for manual processing? How will you get data to the Recovery Operations Center for off-site processing? What will you do if your site is destroyed? And other specifics identified in the skeleton outline, below.

Critical operations and the time frames in which they become critical must be defined and a User Reaction Plan established for each critical business function. These plans must be independent of the master Disaster Recovery Plan, but be directly coordinated with the master plan so all involved are fully aware of the needs and what must be done to meet those needs. Current rerun documentation may be helpful in defining specific requirements. Differences, if any, between procedures to follow for a MINOR DISASTER versus a MAJOR, or even a CATASTROPHIC DISASTER must be noted. These types of disasters are defined on page 2 (attached) of the master Disaster Recovery Plan. In some cases, it is expected that separate "scripts" or checklists should be made for each category of disaster, and a reaction (UREACT) posture identified for each. An outline of required data follows:

\_\_\_\_\_ DEPARTMENT  
USER REACTION PLAN

**GENERAL** (Basic information and concepts considered in the plan)

**RISK REDUCTION** (What you have done or need to do to reduce the potential for a disaster)

**BACKUP PROCEDURES** (Processing procedures, and off-site storage for vital documents and critical data files)

**EMERGENCY OPERATION (UREACT) PLAN**

- 9) Establish a liaison person for contact with the Recovery Operations Center.
- 10) Document the data flow of critical applications for both computer and manual processing.
- 11) Define the critical operations and the critical time frames for them.
- 12) Identify vital documents and critical data files. Provide an inventory list.
- 13) Determine an off-site storage location for these documents and data files.
- 14) Develop procedures for recovery of vital documents and data files from off-site storage location.
- 15) Determine if an off-site office location is needed.
- 16) Develop a recovery checklist for each critical function.
  - a) Determine the level of service available when notified to implement your Reaction Plan.
  - b) Establish a contact point with the Recovery Operations Center.
  - c) Establish a departmental disaster alert recall roster.
  - d) Establish a means of recovering vital records and data files.
  - e) Establish manual processing plan.
  - f) Determine telecommunication needs and backup procedures if no telecommunication is available.
  - g) Determine personnel requirements.
  - h) Determine equipment needs, and a backup source. (Do you rely on a computer system other than Information Technology Services?)
  - i) Establish a training plan.

University of Northern Iowa  
Information Technology Services  
ADMINISTRATIVE SYSTEMS  
DISASTER RECOVERY PLAN

**GENERAL**

A disaster recovery plan is vital to Information Technology Services' management and campus administration in order to insure continuity of computer operations under emergency or disaster situations. Conditions such as extended computer downtime, natural disasters, or criminal action could require implementation of part or all of the plan. To be effective, the plan must be flexible enough to apply under as many conceivable conditions as possible.

When a disaster occurs, a disaster emergency alert is called notifying key personnel (the Disaster Management Team). These individuals meet, make an assessment of the situation, and under the direction of the Disaster Plan Coordinator, incorporate implementation strategies based upon the severity of the problem and the immediate computational needs of the campus administration.

**CONCEPT**

Within the framework of this plan, a disaster is any event which results in an unexpected computer shutdown such that processing must be accomplished at another site for some period of time. The overall plan provides a description of the resources, procedures and decisions required before, during and after such a disaster to insure that the essential daily business and administrative functions of the campus continue in an orderly fashion.

This plan is developed around off-site storage of backup files, and the use of the campus' alternate processing site(s) to carry on critical administrative computing applications. It meets the disaster recovery requirements of a minor or major disaster, as defined below, with the expectation that the primary and alternate processing sites would not both be destroyed in the same disaster occurrence.

**DEFINITIONS**

An INTERRUPTION OF COMPUTER SERVICES is defined as a situation in which the central computer system, or some peripheral component, is down and precludes computing for a period of less than 24 hours. No facility damage has occurred. Such an occurrence is normally covered by day-to-day emergency procedures and close coordination with the system vendor and its maintenance personnel. An example would be minor hardware or software problems, a major file reload, or a head crash on a critical disk. In cases where an application is required before the system can be returned to normal operation, some level of recovery action may be required.

A MINOR DISASTER is defined to be one in which the central computer system(s) can be restored to, or nearly to, normal operational capacity within four (4) days, or earlier if there is a critical time by which a particular software application must be run to completion. Examples would be a system down awaiting parts, a minor fire or flood, or perhaps software problems requiring a minor rewrite. Little or no facility damage would have occurred.

A MAJOR DISASTER is defined to be one in which the computer(s) are expected to be down for more than four days, or beyond the time a critical software application must be run to completion. A long-term loss of administrative computing support at the particular site can be expected. A more extensive fire or flood, a small earthquake, or minor terrorist activity or civil disorder could place us in a position where damage is extensive and could require a new facility or replacement of major computer components or entire systems. The campus, itself, would still be in operation and require administrative computer support.

A CATASTROPHIC DISASTER is defined to be one wherein the operation of the entire campus is disrupted, and there would be no need for computer support until rebuilding took place and normal campus activities could begin again. A major earthquake, all encompassing fire, or extensive terrorist bombings are examples of possible causes.

A MUTUAL AID AGREEMENT is defined as an informal reciprocal agreement with a computer site that has similar equipment, in which each party agrees to provide computing facilities to the other to the extent possible to meet the emergency priority processing requirements outlined in the agreement. Under this type of agreement the host's requirements have priority; thus, access to facilities is not guaranteed for any particular time or application, but the host will do its utmost to provide the necessary facilities at the earliest time practical. Although processing time cannot be guaranteed, limited processing can generally be agreed to within some reasonable time frame, such as within 24 hours after request. The only charges incurred under this type of agreement are normal usage charges, if any, when off-site processing is actually accomplished. The MEMORANDUM OF UNDERSTANDING (APPENDIX III), which can be used for an agreement between two sites, will define any charges to be incurred.

A mutual aid agreement generally is satisfactory only under short term circumstances requiring limited processing. Therefore, it is doubtful if administrative computing could continue even on a limited basis for an extended period under mutual aid. With the two computer sites and systems currently available to the campus, this type of agreement is not a necessity.

### **CONTINGENCY COMPUTER SITE**

Since the completion of the Curris Business Building (CBB) and subsequent move of ITS computers into that building in the Summer of 1990, the UNI campus has had contingency sites for computing. The former administrative computer room located in GIL-255 is available as a contingency site(s). Those rooms have false flooring as well as sufficient emergency electrical power and air conditioning that can be used to complete critical functions until the problem is resolved, and either will also serve as an alternate processing site for the other for minor and major disaster situations.

To begin computing again after a long term catastrophic disaster, where the entire campus is destroyed, the campus administration might be required to support the high cost of a contractual arrangement for a full time "cold" backup computer facility for reinitiating all, or nearly all, computational requirements, both administrative and academic. A "cold" site is one in which air conditioning and power are provided, but the user must have their required computer system installed and operated from that location until their own facilities can be rebuilt. Several companies

provide this service for users of large scale IBM and DEC computer systems. The cost is very high, and alternatives would have to be evaluated as recovery from a catastrophic disaster begins.

### **IMPACT ANALYSIS**

Interruption of computing services for any length of time, when those services are expected to be available, is at least an irritation and can very quickly become a major detriment to the functioning of the University. A survey of key users of the administrative computing system on this campus indicates that the time of the month has much to do with the maximum downtime any particular user can sustain without seriously affecting the daily business of the University. For example, payroll processing leaves little time between the beginning of a pay cycle and the time the money is to be available to the employee, either in the form of a check or a direct deposit to a bank. Thus, if one of the pay cycles is about to begin or is in process, any amount of downtime is critical. But otherwise, perhaps as much as a week of downtime could occur with only minor inconvenience, for that office/function.

**COPIES**

Copies of this plan are available on the web at <http://www.uni.edu/its/ad/policies/disaster.pdf>

The following list of individuals also have a copy:

- UNI Provost
- UNI Vice President for Administration and Finance
- UNI Operations Auditor
- UNI University Secretary
- CIO University of Northern Iowa
- CIO University of Iowa
- CIO Iowa State University
- UNI ITS Directors
- UNI storage vault located off campus.