Humboldt State University

Risk Analysis and
Disaster Recovery Plan

for

University Computing Services

&

Telecommunications & Network Services

Disaster Recovery Plan

Table of Contents

Table of Contents
(continued)

Table of Contents
(continued)

I. Introduction

This section of the Information Technology Services (ITS) Disaster Recovery Plan outlines procedures for the areas of University Computing Services (UCS) and Telecommunications & Network Services (TNS). Given the nature of the disaster, its breadth, and the extent of the damage, UCS and TNS may be the most or least affected. Accordingly, we may find our role to be central or peripheral in the actions being taken.

If the disaster is localized to computing facilities, our role will be central in restoring services we provide to the campus community. If the disaster is broad and affects many areas on campus, our role will be one of support: assessing overall damage and restoring computing services to assist the University's Emergency Operations Center in performing its functions.

The purpose of this Disaster Recovery Plan is to minimize the operational and financial impact of a disaster upon ITS and to return computer access to this department's users in a timely manner. In the event of a disaster, this plan will establish a chain of command that will set in motion a number of activities to be performed by pre-assigned staff members.

University Computing Services (UCS) is responsible for providing the campus community with access to e-mail, as well as providing student access to course work information and databases, campus network access to Meeting Maker, network file

sharing and printing, and backing up the network in UCS. UCS also supports and provides data backup for the Banner software which contains student financial aid data, registration and enrollment records, faculty data and class information. Banner support is provided primarily to the Office of Enrollment Management and Fiscal Affairs. However, the data in Banner is accessed by every department on campus needing student information including Housing & Dining Services, the Student Health Center and the Library. In addition, UCS provides support to Fiscal Affairs for the Financial Reporting System (FRS).

Telecommunications & Network Services (TNS) is responsible for the telephone connections to the campus which permit access to the following: campus switchboard system (PBX); voice mail (telephone message system); IVR (interactive voice response which allows students to receive financial aid and grade information over the phone); Micom equipment (telephone, data, computer connections for the marine lab in Trinidad); Gandalf (for modem and asynchronous communication); the ethernet equipment; and the microwave equipment (dish on Natural History Museum building and Van Matre Hall).

TNS will be working with the Emergency Operations Center (EOC) in the event of a major disaster. Their first priority is to restore telephone communications to the campus.

II. Scope of this Plan

This Disaster Recovery Plan describes the actions that will be taken by specific personnel in University Computing Services and Telecommunications & Network Services to cope with various disasters which might take place on the Humboldt State University campus. It does not address the recovery procedures required by the HSU user community, although computer information made available to them from the UCS department will assist them in their computer recovery process. Each department and area will need to address its own recovery requirements and procedures. UCS offers assistance to these departments and areas in developing their own recovery plans, as well as securing an off-site location for storing their backed up data.

This plan does not define the procedures used by the University to respond to disasters which might affect it as a whole. Those procedures are addressed in the Campus Emergency Management Plan on file in the Emergency Operations Center. However, certain aspects of this plan will work in conjunction with the campus recovery plan, e.g., restoring and/or providing telephone communications and access to vital records via Banner.

III. Definitions

Disaster – A sudden calamitous event bringing potentially great damage, loss or destruction.

Downtime Limit – The length of time the University can be without computing support; this varies depending on the nature of business in each department, i.e., fiscal management, Banner forms, etc., and the necessity for access to the vital records information.

Emergency – An unforeseen combination of circumstances or the resulting state that calls for immediate action.

Risk – The likelihood or probability that a loss of information assets or breach of security will occur.

Risk Analysis – The process of evaluating the vulnerability of information assets to various threats, the costs or impact of potential losses and the alternative means of removing or minimizing risks.

Risk Management – The process of taking actions to avoid risks or reduce risks to acceptable levels.

IV. Classifying Computing Applications

Computing applications can be categorized with the following terms:

Critical – These functions cannot be performed unless the same capabilities (i.e., computer systems) are found to replace the damaged system. Critical applications cannot be replaced by manual methods under any circumstances. Tolerance to interruption is very low and the recovery cost is very high. An example of a critical application includes accessing Banner during student registration.

Vital – These functions cannot be performed by manual means or can be performed manually for only a very brief period. There is a somewhat higher tolerance for interruption, and a somewhat lower cost for recovery, provided that functions are restored within a certain time, usually only a few days. For applications classified as "vital," a brief suspension of processing can be tolerated, but a considerable amount of "catching up" will be needed to restore data to current or useable form.

Non-Critical – These applications may be interrupted for an extended period, at little or no cost to the University, and require little or no catching up when restored. Software applications such as Meeting Maker, used for scheduling appointments and meetings, ArcServe, used for backing up workstations in UCS, and Eudora, used for e-mail, are considered non-critical.

V. Risk Management

Risk management is the process of performing a risk analysis to identify and assess HSU's University Computing Services and Telecommunications & Network Services data and information assets and the threats to them. This process defines a program which can eliminate, or reduce to an acceptable level, those threats and establish the procedures which will be used to recover from threats which cannot be eliminated but can be foreseen. Risk management is based on a division of responsibility among management and staff with written documentation that describes specific responsibilities of each position.

The following identifies three different disaster scenarios and describes the risk analysis and assessment for disasters that could have an impact on University Computing Services and/or Telecommunications & Network Services.

VI. Identification of Disaster Scenarios / Risk Analysis

Humboldt State University is the northernmost campus in the California State University system. We are located in the city of Arcata, 270 miles north of San Francisco, situated between redwood groves and the Pacific Ocean.

We can generally classify threats to information resources at Humboldt State University into three categories:

1) University-wide disasters;
2) localized disaster occurring in Van Matre Hall, Siemens Hall or Natural Resources Building; and
3) a major service loss, resulting from a security or technical threat, such as an Alpha or unit failure or telecommunications equipment failure.

University-wide disasters: Those major catastrophes that affect the campus as a whole. The circumstances of these disasters vary, but are addressed by a campus-wide disaster recovery team. Information Technology Services (ITS) will play a part in the recovery operations, but only as an integrated member of the whole.

Localized disasters: Those events which will affect ITS equipment, facilities and personnel. These would be confined to very limited physical areas, such as Van Matre Hall, Siemens Hall, or the Natural Resources Building, where computing or telecommunications equipment is stored.

A major service loss: An event which creates a technical or security threat such as the power failing to an Alpha server that supplies the campus community with e-mail, internet access, or financial data; or a telecommunications equipment failure. In the event of a major service loss, especially one in which data could be lost, the Rapid Response Team would be activated to resolve the technical or security threat.

A. University-wide Disasters:

University-wide disasters are discussed in the Humboldt State University Campus Emergency Management Plan. Disaster recovery planning for UCS or TNS conforms to this plan so that recovery activities can be carried out on a cooperative basis. TNS will work in coordination with the Emergency Operations Center. Depending on the type and extent of the disaster, its main role will be to restore telephone and data communications to the campus community.

The disasters that could potentially affect the University, and possibly UCS and TNS, are fire, rain or water damage, earthquake, hazardous materials, aircraft collision and bomb threats. Other disasters such as those caused by avalanche, volcanic eruption or nuclear power plant meltdown are virtually non-existent.

There is a nuclear power plant located on a fault line at Humboldt Bay. It was decommissioned approximately twenty years ago, but not dismantled. It continues to be used as a secondary backup power supply. If an earthquake hit

the area, there would be no direct impact from this power plant on Humboldt State University. It could complicate local power supply issues and contaminate the bay, but there would be no contamination in the atmosphere.

Fire

The HSU campus is surrounded and landscaped with redwood trees and foliage. However, forest-type fires around the campus are a rare event. The layout of the campus tends to preclude a fire affecting more than one building at a time. All buildings on campus are equipped with fire alarms and fire extinguishers.

Rain or water damage

During the rainy season, there is always the potential for flooding in outlying areas such as the Arcata Bottoms, Fortuna and sections of Eureka. Although this may affect transportation to the campus, it generally does not affect operations on the campus unless there is water damage due to an extensive amount of rain. Standing water may occur on some campus building rooftops and also in building basements. This could pose a threat to equipment located in basements or vital records stored in lower levels of buildings.

Earthquake

We are located along an earthquake fault line and are prone to experiencing minor to major tremors. Most of these tremors occur offshore and pose little, if any danger. However, approximately every 300 years a major quake has hit this

area. The latest statistics indicate that we are due for a major event, perhaps an 8.0-9.0. A tremor of this scale would isolate not only the campus, but also the city of Arcata. Arcata is linked to other towns north and south via small bridges on Highway 101 and to the east via Highway 299. It is possible that even in a lesser scale event (e.g., 7.0), access to these main roads would be limited to emergency vehicles only, if at all.

Hazardous materials

Arcata is a small, rural area that is generally removed from the risk of a hazardous material threat. Although hazardous materials can be transported along Highway 101 adjacent to this campus, a hazardous materials spill is rare. However, this could be considered a vulnerability due to the close proximity to the campus. Hazardous materials are also kept on campus, but generally in very small amounts.

Aircraft collision

There is one small commercial airport in McKinleyville, north of Arcata. Generally the flight pattern of the small planes operated by Horizon and United Express takes them along the coastline instead of inland. However, occasionally these planes fly over the campus depending on wind direction and visibility. This situation can be a threat to the campus if a plane should lose altitude and crash into Founders Hall, Van Matre Hall or in the nearby Redwood

Bowl. Significant damage and injury could occur to buildings, cars and personnel.

Bomb Threat

A bomb threat is an unusual occurrence. If advanced warning were received by UPD or department personnel, that area and perhaps the entire campus would immediately be evacuated. A bomb explosion could destroy equipment and cause injury to personnel anywhere on campus.

1. Effects of University-wide Disasters on UCS

The HSU Campus Emergency Management Plan addresses some of the threats noted above, and the steps to be implemented in the recovery process. UCS and TNS may be affected by the university-wide threats described above either peripherally or centrally. We would participate in that recovery process according to the disaster scenario and the computing and telecommunications areas affected. The severity of the event would vary with the circumstances, as would the response from each area.

Fire

All major buildings on campus are equipped with fire alarm systems, including the residence halls. Older buildings on campus have hose cabinets for extinguishing fires and 25% of the campus buildings have

sprinkler systems. If a fire broke out on campus, this disaster could affect UCS and TNS in several ways depending on the location of the fire.

First, if the fire were located in Founders Hall, which adjoins Van Matre Hall, but of a scale large enough to be considered a University-wide emergency, our staff would have to be evacuated quickly. There might not be time enough for an orderly shut down of equipment. The main emergency shut-off button in the computer operations center would have to be activated. Second, if a fire occurred in Van Matre Hall, which houses the computer operations center, or Siemens Hall, which houses much of the telecommunications equipment, data and equipment could be destroyed or at the very least be damaged as a result of heat or smoke from the fire. And, third, there is always the potential for data or equipment to be damaged or destroyed in the attempt to extinguish a fire.

Rain or water damage

Flooding due to heavy rain does not directly pose a threat to UCS. Access to the campus may be limited due to flooding in low-lying areas; but water damage to computing equipment is unlikely because the computer center is located at the top of the hill on the second floor. Water levels due to heavy rains are also monitored and measured, so we can expect that TNS would have sufficient warning to protect the equipment located in Siemens Hall basement and prevent the loss of telecommunications support.

Earthquake

If an earthquake impacts the whole campus during business hours, it will also affect computing services and telephone communications. Van Matre Hall is built from solid concrete and steel beams and would most likely withstand a major tremor. But, if an earthquake of sizeable magnitude hit, we will lose power to the building and the Alpha servers, as well as lose telephone communications. If we are faced with a seismically strong earthquake, such as a 7.0 or higher, we might be faced with the total destruction of our computing and telecommunications equipment. If Siemens Hall or Natural Resources are structurally damaged by an earthquake, there could also be damage to the telecommunications equipment housed there as well as limited access to assess the damage and repair it.

Depending on the magnitude of the earthquake, a tsunami warning might occur. Since there may be very little time for an evacuation, staff may be instructed to remain in the building and close all the windows. A tsunami of huge proportions would probably reach the University, but Van Matre Hall is at the highest elevation on campus and may be the safest place.

Hazardous Materials

A sudden release or spill of hazardous materials by a truck traveling on Highway 101 would allow little time for an organized response. People may be advised to stay indoors, with doors and windows shut, to prevent breathing contaminated air. A major off-campus release of hazardous materials could require the evacuation of all or part of the campus. An on-campus incident is unlikely to require an evacuation of more than a very small area. Any injured, exposed or ill persons will be treated at the campus health center or, if necessary, transported to a local hospital. While a hazardous materials spill would not necessarily affect equipment, it may affect the staff who work in UCS and TNS.

Aircraft Collision

Although this has not occurred yet, recent changes in flight patterns could result in an aircraft collision with the campus. If an aircraft en route to or from the Arcata/McKinleyville Airport crashed onto any part of the campus, it could affect the operations in UCS and TNS. Specifically, if a plane crashed in or near Redwood Bowl or Founders Hall, it would most likely have a direct impact on Van Matre Hall. In this scenario, there would be no time for routine, thoughtful procedures. Significant damage and injury could occur to Van Matre, staff members, and automobiles. Staff would be immediately evacuated and their safety would take priority over equipment damage assessment. In such an event, UPD will be

contacting the Arcata Fire Department and possibly local medical personnel for assistance. If there is extensive damage to Van Matre, a mobile recovery site may be utilized until new facilities can be found to house the computer operations center.

Bomb Threat

Although this threat might be limited to the area on campus where the bomb threat is located, it could have an impact on telephone communications or computer operations.

2. University-wide Planned Response

A risk analysis of the above scenarios would normally include recommendations for taking protective measures to eliminate, or reduce to an acceptable level, the threats to Humboldt State. However, it is outside the scope of this Disaster Recovery Plan to include such recommendations here for the entire University. The University's planned response is available in the Campus Emergency Management Plan located in the Emergency Operations Center.

B. Localized Risk Assessments in UCS

University Computing Services and Telecommunications & Network Services (TNS) work in conjunction with each other to provide services to the campus; however, their roles and responses to disaster situations will be different.

This section describes the risk assessment and minimization of disaster scenarios specific to the information resources in University Computing Services. Some scenarios are grouped together because their assessment and effect are likely to be similar.

Rain/Water Damage and Fire

Van Matre Hall is located on the top of a hill overlooking the rest of the campus and the computing equipment is located on the second floor of this building, making it very unlikely that flood waters could reach this level. However, measures have already been implemented to prevent damage to computing equipment should we experience heavy rainfall. The roof on Van Matre Hall has been inspected and repaired and plastic sheeting has been cut to precise measurements to cover each Alpha server in the computer operations room should water manage to seep in. A sensor has also been installed in the computer operations room to detect heat and water. If either of these is detected, UPD is alerted as well as the systems administrator and the UCS manager. Telecommunications equipment is housed in the basement of Siemens Hall which may potentially incur damage if water leaked into this area. Sensors have been placed in this room to alert management and UPD if water is detected.

All campus buildings, including Van Matre, Siemens Hall and Natural Resources (NR) have fire alarms installed and fire extinguishers available. Van Matre also has a smoke detector. Siemens Hall and NR have sensors to alert

UPD and management if smoke is detected where the main telecommunications equipment is housed. A halon fire suppression system has been installed in the computer operations center to safely extinguish fires. Without a chemically based fire extinguishing system, there is the potential for equipment to be damaged as a result of using water to suppress flames.

Earthquake/Aircraft Collision

Van Matre Hall is one of the most secure buildings on campus for earthquake protection. This building is constructed with steel beams and concrete and is anchored approximately 30 feet into the ground. The Alphas and NT servers are on platforms that are securely attached to the floor. A major tremor could result in a campus-wide or localized power outage which would affect computing services to the campus. There is a main power switch in the computer operations center which will turn the power off in case of a blackout. We also have backup batteries to provide ongoing power to these machines for approximately 30-40 minutes, if necessary.

If an aircraft collided with the campus, particularly near Van Matre Hall or Redwood Bowl, there is nothing structurally that can be done to the building or field to protect them against this type of disaster. If the collision occurred, the building would be evacuated and all personnel would be checked for injuries.

Bomb Threat

If we are notified of the possibility of a bomb, UPD will immediately be informed and the building will be evacuated. We will wait until the building has been thoroughly checked by appropriate personnel before reentering the premises.

C. Major Service Losses

Major service losses are emergencies or disasters which would specifically impact University Computing Services or Telecommunications & Network Services. The risks identified here have the potential to affect the technical or physical security of computing services and telephone communications on the campus. These risks can cause physical destruction of equipment and information, temporary interruption of operations and/or inaccessibility.

Theft / Vandalism

These are rare events for UCS and TNS. Because access to the computer operations center is limited, there is little, if any, opportunity for theft or vandalism. Theft and vandalism occur more frequently in the areas of Academic Computing and Media Distribution and are considered the main source of loss for the latter.

Intrusions, Explosives, Terrorism

Access to the computer operations center is very limited. The outside hallway door is always locked and the main entrance inside is accessible only by a keypunch lock. Only appropriate staff members have a key to this area. There is usually a staff member in the computer operations center during business hours. The other entrance is through the front office and inside the office of two staff members. It would be nearly impossible for an intruder to access Computer Operations without being noticed by staff members. The rooms where the telecommunications equipment is housed are equipped with intruder alerts and would send a signal to the University Police should unauthorized access occur.

Mechanical Failure

Mechanical failure is a more likely event than a bomb threat or terrorist act. Mainframe equipment fails periodically and servers become overloaded with processes and prevent users from accessing software or forms. These failures are dealt with as normal circumstances, requiring emergency maintenance which is received from contracted vendors or computing staff.

If an Alpha fails, staff members run diagnostics to determine the problem. If it remains unsolved, we have a maintenance agreement with Hewlett-Packard to assist us with troubleshooting the problem or supply us with a replacement part.

Software Failure

Software malfunctions occasionally occur. These are more probable when the software application is new. Although software is rigorously debugged during its testing phase, it is common for some errors not to be detected until production has begun. When this has occurred, the analysts have always been effective at resolving the problem in a timely manner.

Power Failures

Power failures can come in the form of surges in which too much power is sent on the lines, brownouts in which the power falls below operating levels, and blackouts in which the power is cut off completely. Several events can contribute to power failures including storms, downed power lines and earthquakes.

Telecommunications & Network Services has UPS generators for its equipment in Siemens Hall and the Natural Resources building to use as a backup in case of power failures. This system is also based on redundant applications; in case one function fails, another will be activated to ensure continued service.

UCS equipment is very sensitive to power failures. Each server has a built-in UPS which is programmed to take the system down in an orderly manner should the power outage extend beyond 10 minutes. Depending on the circumstances of the power outage, damage can occur to both the hardware components and

the users' data. In almost every case, once a server has gone down from a power loss, it will require technical staff to bring it back up again and check for damage and data loss.

The damage of a power failure can be severe depending on the cause and length of the outage. Likewise, the amount of time required to bring the system back up varies.

Security Threats

Security threats can be caused by a computer hacker trying to break into the system. Several software programs are currently in use to prevent and detect an unauthorized user's attempt to access files or accounts inappropriately. These threats can occur from on-campus users exploring areas on the system where they should not be as well as off-campus users simply testing their skills. The campus can be hit by a spammer's attack or an unauthorized user can attempt to use our servers to gain access to other ISPs.

VII. Risk Analysis and Minimization for Telecommunications & Network Services

If a major disaster affects the University, one of the first priorities is restoring telephone communications, particularly for health and safety reasons. Restoring the data lines is also important for UCS to restore access to the Banner software, Fiscal Affairs information and for assisting UPD in locating people on campus via Banner.

We are using a self-maintenance agreement with the telephone vendor, Ericsson, allowing us to repair and maintain the equipment. However, we also have a technical service contract with Ericsson ensuring a rapid response to the University in case of emergencies.

Should the telecommunications system incur a major power outage or other significant damage, 30 telephone lines on campus will be immediately switched to the central office in Arcata via the fail safe transfer station. Telephones with the emergency phone numbers have been strategically placed around campus to allow for immediate communication among ITS, the President's and Vice Presidents' offices, Plant Operations, the EOC and Procurement. Additionally, there are a sufficient number of cell phones available in case of emergency. There is also a service agreement with Octel (voice mail service) which states they will commit to assisting us in case of emergency even without following normal paperwork procedures.

VIII. Recovery Activity Analysis

A. Scale of Damage

After describing the threats to which HSU is vulnerable, it is clear that the degree of vulnerability varies depending on the threat. If we attempted to rank the threats, there are several things we could focus on such as the cost of recovery, amount of time the computer systems would be unavailable and the amount of damage the threat could cause.

Rather than focusing on recovery from individual threats, we will base the recovery efforts on a scale based on the amount or level of damage incurred by the threat or disaster. The procedures to recover from minor data loss will be essentially the same regardless of the cause of the loss, e.g., machine failure, human error or power failure. Likewise, the procedures to recover from equipment destruction will be the same whether the destruction was caused by fire or explosive attack.

The scales of damage are as follows:

Total: Physical facilities, hardware and/or data is destroyed, requiring the replacement of equipment and data to recover;

Major: There is extensive hardware and/or data damage, requiring some replacement of equipment and data to recover;

Partial: There is minor damage to hardware and/or data, requiring some replacement of equipment but mostly restoring data; and

Minor: Only data is damaged and only restoration is required to recover.

IX. Data Backup and Off-Site Storage

To protect the vital records data and computer software in UCS from a disaster or major service loss, backup procedures have been implemented and off-site storage facilities have been secured.

Staff work stations in UCS run development software, various diagnostic tools and user support software and are scheduled for back up once per week using ArcServe software. The student information data for the Banner software is accessed from the servers located in UCS and is backed up twice per week. These backup tapes are then stored in the vault located in Founders Hall.

In the event the backup tapes in the vault are inaccessible, lost, or damaged, we have implemented a mutual exchange off-site storage agreement with Sonoma State University in Santa Rosa. This agreement makes it possible for us to send copies of our weekly backups to Sonoma's Information Technology Department on a monthly basis in exchange for storing its data backups. The second week of every month, a taped backup of our Banner and fiscal data records are sent via Federal Express to Sonoma State. If an emergency situation arises and we are unable to reach our on-campus backups, we would be able to retrieve a recent copy of our vital record information from Sonoma State University.

For disaster recovery purposes, a Unix Alpha server is located in the University Police Department's (UPD) Emergency Operations Center (EOC). Banner information is transferred daily to this computer. In case of a major disaster, this server will give UPD access to vital records in a short period of time, i.e., number of classes in session, names of students in each class and identify the buildings and room numbers where classes are being held at the time the disaster occurs. This will expedite the search for people who might be injured as a result of a disaster.

X. Management Recovery Team

The Management Recovery Team (MRT) will coordinate the activities of all the disaster recovery teams. The recovery teams will periodically report to the MRT to provide the status of equipment and data restoration. The MRT is composed of the Emergency Team Coordinator (ETC) for ITS, an ETC for University Computing Services (UCS) and an ETC for Telecommunications & Network Services (TNS).

Following an emergency or disaster, the chain of command is as follows:

1. The Director, ITS, is the ETC-ITS.
2. If the Director, ITS, is not available,

   the Manager, TNS, is the ETC-ITS.
3. If the Director and Manager, TNS, are not available,

   the Manager, UCS, is the ETC-ITS.

Depending on the nature of the emergency or disaster:

the Manager, UCS, may be assigned to the EOC Finance/Administration Section;

the Manager, TNS, may be assigned to the EOC Operations Section.

4. If none of the above-designated personnel are available, one of the following will become the ETC-ITS according to who arrives on campus first:

   a. Manager, Academic Computing

   b. Manager, Instructional Media Services

The Management Recovery Team is composed of the following members:

	Title	Phone
ETC - Information Technology Services:	Director, ITS	x6101
Backup ETC-ITS:	Manager, TNS	x6114
Second Backup ETC-ITS:	Manager, UCS	x6164
Asst. to the ETC-ITS:	Information Security Coordinator	x6117
Alternate Backups for the ETC-ITS:	Manager, Academic Computing	x4201
	Manager, Instructional Media Svcs	x3323
ETC - University Computing Services:	Manager, UCS	x6164
Backup ETC-UCS:	Analyst, UCS	x6151
ETC - Telecommunications & Network Services	Manager, TNS	x6114
Backup ETC-TNS:	Operations Manager	x6131

XI. Responsibilities of the Emergency Team Coordinator for Information Technology Services (ETC-ITS):

1. Alert all staff to be on standby.

2. Make certain that all other emergency teams required for the specific situation are immediately notified and activated.

3. Notify UPD and they will notify any other necessary on- or off-campus emergency operations.

4. Notify Plant Operations that Operations and Technical Support will need their assistance for keys and other access, special equipment, vehicles for transportation on- and off-campus, etc.

5. Prioritize system and application support levels. Systems to receive priority are telephone, data communications, *sorrel* (Web server), *axe* (Email server), *laurel* (Banner), *Polaris* (Domain Name Server), and *jacks* (Fiscal Affairs).

6. Ensure that contact with the Chancellor's Office in Long Beach is made through the EOC to inform them of the nature and extent of the disaster and to coordinate procurement of emergency funds.

XII. Responsibilities of the Assistant to the Emergency Team Coordinator for ITS (AETC-ITS):

1. Have thorough knowledge of the Disaster Recovery Plan and assist the ETC to ensure that all aspects of the plan are implemented.

2. Provide backup support for the ETC in charge and assist with coordinating personnel and recovery procedures.

3. Document changes made to the plan over time and coordinate testing of the plan to ensure a successful recovery after an emergency or disaster.

XIII. Responsibilities of the Emergency Team Coordinator for University Computing Services (ETC-UCS):

1. Bring together team members to assist in restoration or relocation of computing facilities and to assist Emergency Team Coordinator in prioritizing.

2. Establish priorities for Operating Systems Technicians in terms of reestablishing current system or utilizing backup systems.

3. Coordinate with Operations personnel on availability of supplies, tapes, files, special forms, etc.

4. Coordinate with Hardware Technician on extent of damage of current equipment and timeline for restoration.

5. Establish priorities for Application Analysts in terms of setting up Banner/Oracle access.

6. Bring Help Desk Team together to assist in restoring and updating information on ITS web site.

7. Coordinate with academic clients, Help Desk staff and system support the prioritizing and reestablishing of the computing resources.

XIV. Responsibilities of the Emergency Team Coordinator for Telecommunications & Network Services (ETC-TNS):

1. Bring together team members to assist in determining damage assessment and coordinate efforts and priorities with the EOC and Emergency Team Coordinator.

2. Establish priorities for Telecommunications & Network Services Team members and coordinate efforts to reestablish telephone and data communications services for the campus.

3. Assist University Computing Services in establishing communications with UPD and central Alpha servers, i.e., *sorrel, axe, Polaris, jacks, willow* and *laurel*.

XV. Additional Duties for the ETC-ITS, ETC-UCS and ETC-TNS

Depending upon the nature of the disaster, the ETCs will assume a variety of roles not necessarily addressed directly by the DRP.

The ETCs must be ready to handle some of the following:

- Keep in close touch with the Emergency Operations Center. Pursue an alternate evacuation site if the assigned site is not adequate or not available due to unexpected conditions.

- Monitor Computer Center staff to maintain as much stability as possible and to prevent anyone from re-entering the Computer Center building if it is considered unsafe.

- Brief the staff on the situation as it is known. Remind the staff that public statements are not to be made by anyone except appropriate personnel designated by the Public Information Officer (PIO).

XVI. Disaster Recovery Teams

The Disaster Recovery Teams will report directly to the ETCs of the Management Recovery Team (MRT). However, any staff member may become a designated Emergency Team Coordinator. Following a disaster, an officer from the Emergency Operations Center (EOC) will be calling each department to identify staff and locate managers and/or department heads. If none of the designated ETCs are available, the staff member who responds to the telephone call from the EOC may be designated by the EOC as the ETC and assume authority until relieved by a member of the MRT.

The following identifies the Disaster Recovery Teams by staff position with their office telephone extensions (the prefix is 826). For a listing of current staff in each position, see Appendix B, Page 90.

Systems Recovery Team

Operations/Off-site Storage:	Office
Operations Specialist	x6127
Information Technology Consultant	x6117

Operating Systems Technicians:	Office
Unix System Administrator	x6123
Unix System Administrator	x6113
Systems Analyst/Unix Administrator	x6164
Systems Analyst/NT Administrator	x6120

Hardware/Software Support:	Office
Information Technology Consultant	x6112
Information Technology Consultant	x6110
Information Technology Consultant	x6152

Technical Support Team – Banner/Oracle/FRS

	Office
Systems Analyst	x6120
Systems Analyst	x6159
Systems Analyst	x6164
Systems Analyst	x6151
DBA/Systems Analyst	x6119
DBA	x6122

User Liaison Team – Help Desk

	Office
Help Desk Coordinator	x6106
Help Desk Assistant	x6251
Administrative Support Asst. II	x3815

Telecommunications & Network Services Team

	Office
Central Contact Number	x5000
Manager	x5000
Operations Manager	x5000
Instructional Support Asst. II	x5000
University Operator	x5000
Programmer/Analyst	x5000
Network Analyst	x5000
Network Analyst	x5000
Network Analyst	x5000
Network Analyst	x5000
Equipment Specialist	x5000

XVII. Responsibilities of the Disaster Recovery Teams

If a disaster is declared or major damage occurs to UCS or TNS, the disaster recovery teams will be activated according to their roles and responsibilities. If any members of these teams are not available or are called to assist other areas on campus, staff from Academic Computing may be called to assist these teams with the recovery efforts. A contact list for Academic Computing staff is located in Appendix G, Page 101.

- **Systems Recovery Team.**

  Operations / Off-site Storage. This group is assembled when the ETC-ITS decides that interim computing support will be provided at an alternate site within an acceptable time and more quickly than waiting for site restoration. This group will be on-call to retrieve the backup media from the vault or the off-site storage facility (Sonoma State University) and transport them to the alternate site which will either be the Emergency Operations Center or the Mobile Recovery Unit. It is this team's responsibility to contact Sonoma State University Information Technology Department to retrieve backup copies of our vital records database if this becomes necessary. This group also will participate in reoccupation activities. It will work closely with the Information Technology personnel at Sonoma State and the EOC at HSU.

  Operating Systems Technicians. This group restores the system tapes from the backup media whether in the mobile cold site or Van Matre Hall. It loads

and tests the operating systems and any associated software and data files on the Alphas and/or NT Servers. If vital areas of the campus are in need of accessing computing services and vital information, it will follow normal procedures to bring the servers back online and begin restoring data and computing services on a limited basis. This group will test the restored system with standard diagnostics and will continue to provide support, perform operating system modifications, install corrective codes, and tune the system until it is restored to normal.

The most critical applications will be established first such as access to student records and fiscal information. The applications are prioritized as follows:

Alphas

1.	*Polaris*	Domain Name Server
2.	*sorrel*	Web server for system status update
3.	*willow*	Oracle databases
4.	*laurel*	Banner/Student Information System
5.	*jacks*	Fiscal Affairs data
6.	*axe*	E-mail

NT Servers

1.	*Aspen*	ArcServe backups; print serving and file serving
2.	*Elm*	Banner forms
3.	*Web Mail*	Web Mail
4.	*Madrone*	Meeting Maker; anti-virus updates; search engine

If any of the above-listed NT servers need to be replaced, the ETC-ITS will contact the manager of Academic Computing to request appropriate PCs from the computer labs to be used as NT servers.

Hardware/Software Support. This group will assist with setting up workstations and installing appropriate software programs on the PCs in the alternate site. It will also provide backup support for the HSU Webmaster. An alternate HSU Web page will be maintained and, in an emergency, will include appropriate emergency information such as the status of classes, the campus, and response to the event. If the EOC Public Information Officer deems it appropriate, the alternate HSU Web page will be displayed on the Internet following a campus emergency or disaster.

In addition, this group will provide technical workstation assistance on a priority basis to the following areas that work with vital information:

Public Safety/Emergency Operations Center

Fiscal Affairs

Office of Enrollment Management

Student Health Center

Plant Operations

Public Affairs

Executive Committee locations

- **Technical Support Team – Banner/Oracle/FRS.**

  This team must immediately familiarize itself with the environment in the alternate site and apply their old tasks to the new equipment. While systems and applications recovery are being accomplished, the Technical Support Team supports these activities. It remains on the site and operates the center at emergency service levels, accommodating both the normal application processing of the University departments it supports and also scheduling time for the User Liaison Team.

  The alternate site might be a Mobile Recovery Unit or the Emergency Operations Center. If Technical Support is moved to an alternate site, it will be done on a shift basis when it is determined how many staff members will be needed at the alternate site and how many will remain for recovery operations in the Computer Center in Van Matre Hall.

- **User Liaison Team – Help Desk.**

  This team will work with the users to assist them in accomplishing their restoration in the most efficient manner possible. It will coordinate its activities with the Technical Support Team and the Systems Recovery Team to see that the most recent data files are available and brought to the operational state they had prior to the disaster. It will monitor the status of the system and its applications and continue to update that information for users as necessary and appropriate.

- **Telecommunications & Network Services Team.**

  This team will take direction from the EOC. After determining where the system is down through the diagnostic process, it will begin procedures to restore service with the cooperation of Plant Operations, Pacific Bell and contracted vendors, as appropriate. It may also work in coordination with the Systems Recovery Team to assess the status of the network, estimate the downtime and restore access to the data lines which will bring computing services back on-line.

XVIII. Additional Responsibilities of the Disaster Recovery Teams

In addition to the above-mentioned responsibilities, and depending upon the nature of the disaster, some members of the Disaster Recovery Teams might be called upon to offer assistance, on a priority basis, to other campus departments that work with vital information.

These departments are as follows:

Public Safety/Emergency Operations Center

Fiscal Affairs

Office of Enrollment Management

Student Health Center

Plant Operations

Public Affairs

Executive Committee locations

XIX. Scale of Damage / Disaster Scenario

We have already identified three disaster scenarios: campus-wide, ITS, and major service loss. This section will describe the procedures we will follow depending on the scale of damage as it applies to each disaster scenario.

Just as fire or explosion might have similar recovery procedures, within these events the range of disaster could vary. A small fire that can be put out by a staff member with a hand-held extinguisher will produce damage on a minor scale. A large fire could potentially cause significant damage to equipment and office space.

A. University-Wide Disasters

Total Disaster or Major Damage: If the scale of damage from the emergency is determined to be a total disaster or major damage has occurred to more than one building on campus, then UCS and TNS will most likely be affected. This type of university-wide damage would probably result from a major earthquake. In this situation, the MRT will take direction from the Campus Emergency Management Plan and keep the disaster recovery teams informed in UCS and TNS. If the disaster occurs campus-wide, the Telecommunications & Network Services Team will receive instructions from the EOC.

Emergency Operations Center: Campus recovery procedures will originate from the Emergency Operations Center (EOC). If data communications are

down on the campus, an Alpha server is available in the EOC to access student files and financial data. The data on this server will assist the Director of the EOC in locating students and faculty who might have been in class when the disaster occurred. Once people are accounted for, access to the student records and financial information will be available to Office of Enrollment Management and Fiscal Affairs on a limited basis.

Partial or Minor Damage: If the scale is determined to be only partial or minor damage, this may affect only certain areas of the campus. If UCS or TNS has been affected, then the ETC-ITS will determine if an emergency should be declared for this department. At that time, the MRT will follow the procedures appropriate to the situation. If an emergency is declared, the MRT will notify the appropriate recovery teams involved to begin emergency recovery operations.

B. UCS & TNS Disasters

Total Disaster: At this level, computing resources are damaged beyond recovery, requiring the replacement of equipment and data. The offices or building will have received heavy damage and major physical repairs will have to be made before the building will again support computing and telecommunications services.

Because of the time involved in replacing the equipment and in restoring the data, recovery at this level will require either the suspension of computing support for an extended time or the use of alternate facilities. In this scenario, the departments supported by UCS (in particular, Office of Enrollment Management and Fiscal Affairs) would most likely delay their procedures until the system was again on-line because of the current dependency on the Banner software to accomplish their tasks.

If a total disaster occurs only to Van Matre Hall, the ETC-ITS will invoke the Disaster Recovery Procedures. He will then notify the appropriate campus personnel and initiate the request for the alternate site.

1. Mobile "Cold" Site

If we were to experience total destruction or major damage to our building, we would require alternate facilities. Due to our geographic remoteness from other CSUs and the unpredictable road conditions, it would be extremely difficult to travel to another location to use computing equipment or access our data. Instead, we have contracted with a commercial vendor, Rentsys Recovery, to provide us with a mobile “cold” site in the event we are unable to occupy our building.

A mobile cold site is a fully configured, self-contained data processing facility for use as a user work area during times of recovery from a

disaster. In the event a disaster is declared and assessments to our equipment and building indicate our resources will be unavailable for an extended period of time, the ETC-ITS will notify Rentsys Recovery to deliver the mobile cold site to HSU. If necessary, Hewlett-Packard will also be contacted to deliver the Alphas that are covered in the Recover-All agreement. The estimated delivery time for the mobile unit and the Alphas is within 72 hours.

The staff members on the disaster recovery teams will follow their procedures to bring the servers back online in the mobile cold site and begin restoring data and computing services on a limited basis. The most critical applications will be established first such as access to student records and fiscal information. The applications are prioritized as follows:

Alphas

1. *Polaris* Domain Name Server
2. *sorrel* Web server for system status update
3. *willow* Oracle databases
4. *laurel* Banner/Student Information System
5. *jacks* Fiscal Affairs data
6. *axe* E-mail

NT Servers

1. *Aspen* ArcServe backups; print serving and file serving
2. *Elm* Banner forms
3. *Web Mail* Web Mail
4. *Madrone* Meeting Maker; anti-virus updates; search engine

If any of the above-listed NT servers need to be replaced, the ETC-ITS will contact the manager of Academic Computing to request appropriate PCs from the computer labs to be used as NT servers.

Major Damage: Lack of facility damage is the major difference between total destruction and major damage. Major damage means there may be some structural damage to the building but it can still be occupied. It is not as severe as a disaster causing total destruction. Equipment has mainly suffered from the disaster and there is a possible loss of data. A mobile cold site will not necessarily be needed.

If major damage occurs, the MRT will ask the emergency recovery teams to assess the damage and estimate the timeline to recover equipment and data. The procedures for recovery are very similar to that of a total disaster, but the time frame is shorter because of the availability of the facilities. The damaged equipment will have to be repaired by technical staff or replaced by Hewlett-Packard through our Recover-All maintenance agreement. Data loss will be

recovered either from backup tapes in the vault or mailed via overnight delivery from Sonoma State University.

Partial or Minor Damage: If partial or minor damage occurs to University Computing Services or Telecommunications & Network Services, each staff member will follow his/her normal operating procedures to restore the equipment and the data. This usually will not affect the rest of the campus and will cause little if any downtime. This level is not considered to be an emergency or disaster.

Partial damage is characterized by minor damage to hardware and/or data. Recovery might require some replacement of damaged equipment but will mostly involve the restoration of data. Hardware damage is usually confined to equipment components rather than total loss of devices. Recovery will most likely involve the use of diagnostic software to determine the location and level of the failing component, replacing it and resuming services. In many cases, the system will remain in operation while the repair is made, particularly since the damage will only affect one part of the system.

If there is data loss from the partial damage, data restoration will take place from the backup tapes in the vault or received via overnight mail from Sonoma State.

Minor damage is characterized by loss of data. This could occur as a result of a power outage and the failure of the backup batteries. While the recovery process may be time consuming, backup tapes are readily available and there will be very little if any system down time.

C. Major Service Loss

Total Disaster: A total disaster would indicate damage to the building and equipment. In the event a total disaster occurs in Van Matre Hall, the response will be similar to that of ITS.

Major Damage: Major damage indicates equipment has been damaged and data may be lost. Again, procedures for recovery would be similar to those for major damage occurring to ITS. However, if it is due to a security or technical threat, the Rapid Response Team will be activated to resolve the problem. These problems might occur anywhere on campus, for example, a complete computer shut down during registration or a hacker attempting to bring down the servers resulting in major network problems.

The Rapid Response Team, composed of staff with the expertise to handle the particular situation, would be called upon to assess the damage and restore service. Security and technical threats which require immediate attention and will initiate a Rapid Response from ITS staff meet the following criteria:

1. A single or repetitive event which compromises or threatens to compromise the administrative, operational, or physical security of the campus;

2. An event or attack originating from an HSU site and compromises or threatens to compromise the security of an off-campus site;

3. Has the potential to cause or threaten to cause serious legal ramifications to the University (through the University's network system);

4. Affects or has the potential to affect a large segment of the campus.

Priorities for responding to technical and security threats can be determined by the following means:

Immediate:

- By the criteria set for a rapid response, i.e., poses a security or technical threat.
- By the number of calls showing trouble in a common area, (i.e. OEM during student registration, Financial Aid during loan disbursement, etc.) thereby impacting a large number of people.
- By the determination that a major function (server, lab, power supply) is not working.
- An incident that is time-critical.

High:

- Potential to impact a department or small group of people (in a lab for example).
- Time critical but not as urgent.
- Potential for a security breakdown.

Medium-Low:

- One person is experiencing minor problems (such as receiving inappropriate e-mail, e.g., pornography, spamming, etc.).

A medium-low priority can develop into a high priority if the trouble escalates.

Partial or Minor Damage: In the event that partial or minor damage occurs to UCS or TNS in Van Matre Hall, staff would conduct their routine assessments to determine the extent of the damage and proceed in fixing it.

XX. Notification Procedures for Emergencies or Disasters

If the emergency occurs during business hours, **staff will immediately notify the ETC-ITS** if any of the following occurs:

Fire is suspected

Bomb threat is received

Electrical failure occurs

Water leak

Damage occurs due to earthquake

The person detecting the emergency should use as much discretion as possible under the circumstances to minimize the possibility of creating chaos among others in the vicinity.

The ETC-ITS is authorized and responsible for the following steps:

1. Initiating emergency reporting
2. Initiating damage control
3. Notifying UPD of the disaster or threat
4. If life threatening, take immediate action including evacuating the building and notifying the University Police Department

XXI. Procedures to Ensure Personnel Safety

Once an event has occurred resulting in either total destruction or major damage, the first priority is to make sure all personnel are safe and accounted for. **Staff safety is the first priority.**

If the damage is the result of a hazardous materials release or major storm, the emergency response would be as follows:

- Staff should remain inside the building
- Doors and windows should be secured
- Curtains or mini-blinds should be closed to shield from flying glass
- Staff should take shelter in the hallway if necessary
- Evacuation of the building is a last resort and should be done only under the direction of the ETC-ITS or notification by UPD

If the damage is a result of an earthquake, fire or explosion, the building may have enormous structural damage or be in the process of crumbling. It may be necessary to evacuate the building immediately until it can be declared safe for occupancy. If this is the case, procedures should be followed under Building Evacuation, Page 59. Those who are able must evacuate all personnel and attempt to locate anyone who might be trapped under rubble or debris.

In the event of Fire/Explosion/Bomb Threat, the emergency procedure would be the following:

- Evacuate staff as quickly as possible
- Request assistance from UPD
- Have staff wait at Emergency Assembly Point
- Designated staff to be relocated to Emergency Operations Center
- Designated officer (UPD) will be assigned to secure facility
- Remaining staff members will be released from work and are to leave the area immediately

If the emergency or disaster did not occur in the vicinity of Van Matre Hall and it is safe to remain in the building, check for telephone communication. If the phones are out, the Telecommunications & Network Services Team will check the equipment and attempt to determine when service will be restored.

If telephone service is down, the ETC-ITS will use the emergency phone in the office of the ETC-TNS to check in with UPD and learn the status of the rest of the campus.

After confirming our status with UPD, the Systems Recovery Team will check the status of the systems. This team will determine what servers are functioning and estimate the downtime for those that are damaged.

A. Building Evacuation:

1. The building will be evacuated upon notification by UPD, the ETC-ITS or if there is a life threatening incident or disaster.
2. Pay attention to all marked exits from the area and the building.
3. Walk quickly to the nearest exit and leave the building.
4. Once outside, **proceed to the Emergency Assembly Point**. Do not leave the area. It will be necessary to conduct a roll call to make sure everyone is safe and present.
5. Do not return to the building until directed to do so by either UPD or the ETC-ITS.

B. Emergency Assembly Point:

The Emergency Assembly Point (EAP) is a large, open area, away from power lines, falling debris and other hazards where people can assemble to be accounted for, receive minor first aid, receive instructions and obtain information.

If there is a designated person in charge at the EAP, check in with that person and wait for further instructions. If there is no designated person, remain calm and assist others until a designated person is assigned. Everyone should be accounted for. If anyone is missing, the UPD should be called and a search party activated by the UPD to locate the missing person.

Team members carrying pagers and cell phones might be called upon to assist with disseminating instructions and relaying emergency information at the EAP.

The EAP for staff working in Van Matre Hall at the time of disaster is Redwood Bowl behind Van Matre Hall. If this site is not available because of the nature of the destruction, staff should proceed to the nearest EAP using extreme caution, staying away from buildings where falling debris and glass could present a danger.

XXII. Procedures to Secure Facility

Securing Van Matre Hall is to be implemented in three stages:

- Building Damaged. Depending upon the severity of the emergency and the destruction involved, the MRT will issue instructions to staff on immediate actions to take and will activate emergency team members to determine any injuries that might have occurred and assess damage.

- Building Evacuated. If damage is severe, the MRT will immediately activate disaster recovery teams to assess the situation and equipment. In the event of possible structural damage due to fire or earthquake, the ETC-ITS will direct all personnel to evacuate the building immediately.

- Building Being Repaired. UPD and Plant Operations will activate appropriate personnel and agencies to begin the process of closing down the building until the extent of the damage and timelines for repair can be assessed. The building will remain closed until UPD and Plant Operations gives authorization for re-entry.

Once the building has been evacuated and closed down, the ETC-ITS will:

1. Post Team Members (or UPD officers) near all entrances to prevent staff who might be unaware of the situation from entering the building.

2. Brief UPD officers of the situation upon their arrival to the building. UPD or the Director of Public Affairs will be the source of information to the public.

3. Report to the Emergency Operations Center if the disaster involves the entire campus.

XXIII. Damage Assessment and Recovery Activities

During Business Hours

If the emergency or disaster occurs during business hours, the following procedures will be followed. After either experiencing the disaster or receiving notification of the possible emergency situation, the MRT will direct the disaster recovery teams to conduct an assessment of the damage to the computing and telecommunications equipment and determine how much data has been lost or damaged, and estimate the system or network downtime.

Based on that information, the MRT will determine the severity of the damage, the probable cost, the timeline to repair and the best recovery path. Depending on the nature of the emergency and the time of academic year it occurs, the MRT will determine if the downtime is within an acceptable time frame. The downtime will include estimates of the time required to repair the site, salvage the equipment and/or acquire replacement equipment.

The ETC-ITS will use the disaster scales previously identified and the information from the recovery teams to determine if the emergency qualifies as a disaster and if the disaster recovery plan should be invoked.

If the emergency falls into the categories of partial or minor damage, there is no reason to invoke the disaster recovery plan. These situations can be handled by normal operating procedures.

If the emergency meets the disaster criteria either by the extent of the damage or by the length of estimated downtime, the ETC-ITS will inform the Emergency Management Organization of the need to invoke the disaster recovery plan. After informing the Emergency Management Organization and receiving authorization, the ETC-ITS will then invoke the disaster recovery plan, assemble and inform the disaster recovery teams of the situation and notify appropriate University and vendor personnel.

XXIV. After Business Hours Emergency Response

If the emergency or disaster occurs after business hours or on weekends, UPD will be the first to respond. If the emergency involves the telecommunications system, UPD will follow the calling tree instructions per the TNS Alarm Response Procedures, Page 67.

If the emergency involves ITS or specifically Van Matre Hall, UPD should notify the personnel on the Management Recovery Team in the order listed in Appendix A, Page 86. If the ETC-ITS is not at home or is unreachable, continue calling down the list until a person is reached.

The first ETC responding will come to the campus to determine the severity of the damage. Depending on the nature of the emergency, the ETC will notify the appropriate Disaster Recovery Teams (DRT). The ETC will also attempt to locate and notify the other members of the MRT. The DRTs will conduct an assessment of the damage to the computing and telecommunications equipment and determine how much data has been lost or damaged and the estimated system or network downtime.

Based on that information, the ETC or MRT will determine the severity of the damage, the probable cost, the time line to repair and the best recovery path. Depending on the nature of the emergency and the time of academic year it occurs, the MRT will determine if the downtime is within an acceptable time frame. The

downtime will include estimates of the time required to repair the site, salvage the equipment and/or acquire replacement equipment.

The damage assessment, timeline determinations and recovery activities will be the same as those that take place during business hours.

XXV. Telecommunications & Network Services Alarm Response Procedures

There is a communications alarm indicator panel in UPD to alert personnel that there is a problem with the telephone or data communication system. When an alarm is triggered, a bell will sound to alert the dispatcher. The bell can be turned off by toggling the switch under the alarm panel; however, the lights will stay on until the alarm condition is cleared. During Red and Yellow alerts, which indicate telephone system faults, it is recommended that the Central Office Line, 822-1572, be used to bypass the campus telephone switch.

Dispatchers will be notified by Telecommunications & Network Services staff when the alarm condition is over. The dispatcher should then return the bell switch to the armed position.

During campus business hours, all alarm conditions will immediately be reported to ext. 5000. **After campus hours**, the personnel on the list below should be called in the order listed until direct contact is made. If an answering machine picks up, a message should be left with the time and condition and then the next alternate number should be called. If a pager is called, place the page and then continue to the next person on the list.

Yellow Alert: PBX condition requiring contact of technical staff.

Continue calling down the list every 15 minutes until direct contact is made.

	Phone
Gary Peters	826-6139
Ron McFadden	826-6145
Cliff Schall	826-6114
Jane Hansen	826-6131

Red Alert: **Serious** PBX condition requiring **immediate** contact of technical staff. Continue calling down the list until direct contact is made.

	Phone
Gary Peters	826-6139
Ronn McFadden	826-6145
Cliff Schall	826-6114
Jane Hansen	826-6131

If unable to reach the technical staff after 30 minutes, contact:

Bill Cannon	826-3815

White Alert: Data communications system fault.

	Phone
Ben Curran	826-6130
Rick Garcia	826-6137
Dave Budde	826-6115
Cliff Schall	826-6114
Jane Hansen	826-6131

XXVI. Telephone Use During Emergencies

Emergency Calls Only

After a disaster, especially earthquakes, there is usually a high volume of telephone calls. It is important that you limit phone calls to emergencies only.

Do not call "9-1-1" or the police for confirmation of an earthquake. Listen to the local radio or television stations for information.

Blocking

In cases of extreme congestion of the telephone network, Pacific Bell and/or long distance carriers may institute blocking. Blocking prevents overloading the system by diverting some calls to recordings, allowing other calls to complete.

If you need to place an emergency call:

1. Make sure receivers of all extension phones are on the switch hook (i.e., make sure phones are 'hung up' completely).
2. Stay on the line. You may not hear a dial tone immediately; the delay could be as long as a minute or more.
3. Do not repeatedly depress the switch hook, as this will further delay your call.
4. If you receive a 'fast busy' or 'all circuits are busy' recording, hang up and try again.
5. If physical damage occurs to Pacific Bell equipment or facilities or home/office wiring, it may not be possible to complete the call.

XXVII. Telecommunications & Network Services Disaster Recovery Assistance

Telecommunications & Network Services uses the Octel Overture 350 system for voice mail. In case of disaster, this system includes a backup of system databases, mailbox profiles, subscriber-recorded names and greetings, recorded NameNet names and voice applications messages. It also supports backup for key subscriber voice and fax messages selected by class of service. This provides fast and efficient recovery of critical system information and messages in the event of a natural disaster or other catastrophe.

The server manager can schedule each tape backup to run unattended. If a backup is unsuccessful, the System Backup and Restore sets a non-service-affecting alarm.

Disaster Recovery service for the Octel Overture 350 commits that Octel will use its best efforts to ship replacement parts in an expedited time frame (within 24 hours or less) in the event the server suffers from a major disaster. When requested by the customer, Octel will waive delivery schedule priorities to the extent permitted by prior contract obligations, and commitments and laws and regulations. The price for the replacement product will be the then-current List Price less any applicable discounts.

XXVIII. Procedures for Each Disaster Scenario

A. Fire

1. If possible, determine where the fire is located.
2. If the area is filled with smoke, leave the area for a safer location.
   - call UPD and notify the ETC-ITS
   - stay out of the area until the smoke has cleared and the area is secured
3. If the fire is not out of control and you are not in danger:
   - trained staff should use the fire extinguishers if it is safe
   - sound the fire alarm
   - call UPD and notify the ETC-ITS
4. If the fire is out of control, evacuate all personnel from the area.
   - immediately notify the ETC-ITS and UPD.
   - sound the fire alarm
   - stay at least 300 feet from the area.
5. When the alarm has sounded or if directed to do so by UPD or the ETC-ITS, everyone will walk quickly to the nearest marked exit and leave the building.
6. Once outside, proceed to the Emergency Assembly Point (Redwood Bowl). Do not leave the premises. Roll call will be taken to ensure everyone is safe. Make room for emergency vehicles that may need access to this area.

7. Do not return to the evacuated building unless directed to do so by UPD or the ETC-ITS.

B. Earthquake

1. Move away from the windows and any other glass or objects that could shatter or topple over.
2. Get under a solid object (desk, table, etc.) or brace yourself in the door jam.
3. After the shaking subsides, check for injured people and make certain that all personnel are accounted for.
4. Check for fires, smoke, leaking water, equipment damage and building damage.
5. If damage to the building is severe and is life threatening, everyone will walk quickly to the nearest marked exit and immediately leave the building.
6. Once outside, proceed to the Emergency Assembly Point (Redwood Bowl). Do not leave the premises. Roll call will be taken to ensure everyone is safe. Make room for emergency vehicles that may need access to this area.
7. Do not return to the evacuated building unless directed to do so by UPD or the ETC-ITS.

C. Explosion, Airplane Crash, or Similar Incident

In the event of a violent incident such as a bomb explosion or aircraft colliding near or on the campus that could render the building or area unsafe, take the following action:

1. Immediately take cover under tables, desks, and other such objects for protection against falling glass and debris.
2. After immediate effects of the explosion and/or collision subside, notify UPD and the ETC-ITS. Give your name and the nature and location of the emergency.
3. If necessary or if directed to do so, activate the building alarm.
4. When the alarm has sounded or if directed to do so by UPD or the ETC-ITS, everyone will walk quickly to the nearest marked exit and leave the building.
5. Once outside, proceed to the Emergency Assembly Point (Redwood Bowl). Do not leave the premises. Roll call will be taken to ensure everyone is safe. Make room for emergency vehicles that may need access to this area.
6. Do not return to the evacuated building unless directed to do so by UPD or the ETC-ITS.

D. Telephone Bomb Threats

1. Keep the caller on the line as long as possible.
2. Record every statement spoken by the person making the call.
3. Be sure the caller provides information regarding the location and time of detonation.
4. Ask for the person to repeat the message or verify the information with the caller.
5. If possible, place the caller on speakerphone so that other staff may assist in verifying information.
6. After hanging up, immediately notify UPD at x3456.
7. Inform the others in your area of the threat. Contact the ETC-ITS and Building Coordinator immediately. The decision to evacuate will follow.

E. Smoke

1. If the amount of smoke is minimal, determine the cause.
2. Power-off the equipment that is causing the smoke.
3. If smoke is billowing, leave the area immediately. Protect yourself and other staff at all costs.
4. Shut off the power to the computer room.
5. Call UPD and notify the ETC-ITS.

F. Injuries and Medical Emergencies

When an injury or medical emergency occurs, follow these procedures. For more information, see Appendix K, Page 105.

1. Call UPD for emergency medical assistance, 9-1-1.
2. Make certain the person is breathing. If not, check to determine that the airway is not blocked by the person's tongue or foreign object.
3. Check the person's pulse. If no pulse is felt, administer CPR.
4. Check for severe bleeding after you are sure the victim is breathing and has a pulse.
5. Press a sterile gauze dressing or the cleanest cloth available firmly over the wound and hold it there until the bleeding stops.
6. When the bleeding stops, bandage the dressing firmly in place.

XXIX. Reoccupation Activities

After a disaster has occurred and the building has been repaired, the staff in University Computing Services and Telecommunications & Network Services will be able to reoccupy Van Matre Hall.

Re-occupation activities utilize the same team structure as recovery activities. Many of the things previously done to move to an alternate site must be done again to move back. When the Management Recovery Team receives word that the site is ready this means the following has occurred: All physical repairs to the building have been completed sufficient to allow re-occupation, the electricity has been restored, hardware has been installed and is in working condition, data restoration activities are completed, and the network is ready to resume support of user access.

Once the building is ready to be re-occupied, the MRT will assemble the recovery teams to rebuild the computer systems. The Systems Recovery Team will bring the system back on-line and check the Alphas and PCs; the Technical Support Operations Team will reinstall, if necessary, the Banner software and restore the database; the Operations Emergency Team for Off-site Storage will use the backup tapes to assist the Technical Support Operations Team with their recovery; and the User Liaison Team will assist the campus community with restoring and rebuilding their files and to begin normal operations.

If interim computing has been going on at an alternate site, the re-occupation task is easier. When the ETC-ITS receives notification that Van Matre Hall is ready to be occupied, the MRT will direct the Operations Emergency Team to prepare full system backups on all servers to be transported back to the Alphas and PCs in University Computing Services. These backup tapes will then be stored in the vault and a new copy forwarded to Sonoma State University. The campus systems will then be restored to current status. The users will then be able to continue the activities on the restored equipment. The emergency services levels will be gradually replaced by normal operating procedures. The disaster recovery will be complete.

XXX. Disaster Recovery Plan Maintenance

A disaster recovery plan needs to be maintained. It cannot be assumed that all future disasters will neatly fit into the plan's sections. Computing functions change over time, in some cases drastically. The plan designed to preserve or restore these functions needs to change with them. Changes to the plan will be introduced in three ways:

1. Through change management
2. As a result of plan tests
3. As a result of plan failure during actual disasters

A. Change Management

Change management and periodic testing are the most useful methods of plan maintenance. These methods will come through the Information Security Coordinator (ISC). This person will be responsible for identifying those computing functions and staff assignments that have changed and determining if these changes require a plan update. These changes include equipment revisions for the mobile cold site that need to be relayed to Rentsys Recovery.

The elements in UCS's computing environment that are likely to change most often are data elements and software application upgrades. The ISC needs to ensure the continuity of archived data and that backup and off-site storage procedures are adequate to safeguard these archives. Hewlett-Packard will also

need notification of additional hardware requirements and initiate contract changes if appropriate.

Major modifications or additions to the software applications need to be documented and investigated to gauge their impact on the recovery procedures. New software may have significant impact on backup storage.

Also, personnel turnover will affect the membership of the various teams. As this occurs, the ISC must make the necessary changes to the plan and must see that new staff are trained in their special recovery duties.

B. Plan Testing

It is very important to test the plan before an incident occurs, rather than discover in the process that certain elements just do not work. Testing can occur on a regular basis to keep staff current on procedures, or it can be conducted in drills without prior notification.

Some methodologies of plan testing include:

- Testing sections separately or the entire plan as a unit;
- Involving only the UCS and/or TNS staff, or other areas as well;
- Involving UPD and University officers to add financial concerns; and
- Testing in real time or in a compressed time frame.

It is the intent of ITS to conduct biannual drills with UPD personnel to add unexpected elements to the decision-making process. A scenario will be decided in advance, a situation will be invented that simulates an appropriate disaster, and all the implications of the situation will be tested. The ISC will identify the staff to be involved in the drill, explain the scenario to the staff in advance, identify the objectives of the emergency situation and encourage the staff to watch for unexpected events.

After the drill, the test results will be documented. Where deviation from the plan was required to accomplish a particular task, this will show where changes need to be made in the plan itself. The successful outcome will show that the objectives of the situation are met in a timely manner and we are able to achieve a quick recovery.

C. Plan Failure after a Disaster

This method is the least desirable and should not occur if the plan is tested and staff understands their responsibilities. It is unlikely that a plan will fail completely; however, it is possible that aspects or procedures will require changing as a result of a real-life disaster. We expect that with training, testing and logical procedures, a successful recovery will be achieved.

XXXI. Emergency Preparedness

University Computing Services and Telecommunications & Network Services will conduct biannual drills involving item storage and building evacuation.

A. Training for Emergency Preparedness

It is the responsibility of the ETC-ITS to ensure that all staff members are aware of the risk analysis that has been done regarding UCS and TNS and the recommended methods for responding to the various disasters described.

As part of the Disaster Recovery Plan, all staff members will be familiar with:

1. The overall plan of action
2. The team structures and calling trees
3. The logical activation of each team and their responsibilities
4. Evacuation procedures from the building

Teams will meet on a bi-annual basis to address recovery from various situations ranging from minor to major disasters. A mock disaster might be implemented or role played to determine gaps or flaws in the plan and allow for adjustments in the plan. The staff calling trees and responsibilities will be reviewed on a regular basis to ensure that all personnel identified are up-to-date and fully trained in their areas of responsibility.

XXXII. Release of Information to the Public

A. Loss of Data

When the Emergency Team Coordinator – ITS is notified on an incident which results in the loss of data (e.g., destruction of data itself or physical damage to the computer hosting it), the ETC-ITS will activate the appropriate emergency response protocol and do the following:

1. Notify UPD if the loss appears to be the result of deliberate action.
2. Assess the damage and take steps to limit further loss.
   - In the case of data loss not resulting from hardware damage, take the compromised server down until "hole" is patched.
   - In the case of data loss resulting from hardware damage, bring the server or its replacement/substitute back into operation as per standard emergency response.
   - Restore to service from last good full backup.
3. Form a team consisting of at least one representative from each of ITS, the data owner (e.g., OEM, Human Resources, Housing), and University Communications to prepare public announcements throughout the incident. If a criminal investigation is underway, information must be vetted by UPD prior to release, in consultation with ITS and others as appropriate, to prevent compromise of security. Public announcements and releases should include the following:
   - General what, when, where, who is affected, how, and, if possible, why.
   - What data is lost (non-recoverable).
   - What action impacted parties should take (e.g., reentering the data).
   - What is the current status of compromised system.
   - Other appropriate questions and concerns.

4. Release the information via appropriate channels to the appropriate bodies.

   - Personal contacts by either ITS or the data owner if the number of impacted individual parties is limited.

   - Chancellor's Office if data loss affects University reporting to the CO as determined by the data owner.

   - Executive Committee if the data loss affects the operation of the University as determined by the data owner, ITS, or University Communications.

   - General public announcements (including to targeted constituencies), coordinated by University Communications. These might include bulk e-mail with reference to Web page and FAQ, link on campus homepage, press release to local media and/or a public forum.

5. Perform follow-up to review users' needs and analyze internal department practices.

B. Compromise of Data

When the Emergency Team Coordinator – ITS is notified on an incident which results in the compromise of data (e.g., unauthorized access to data such as protected data for an employee or student), the ETC-ITS will activate the appropriate emergency response protocol and do the following:

1. Notify UPD. Any action that results in the compromise of data should be investigated as a potential criminal act.

2. Assess the damage and take steps to limit further loss:

   - Take the compromised server down until "hole" is patched.

   - Restore to service from last good full backup.

   - Notify the Executive Committee.

   - Notify the Chancellor's Office.

3. Form a team consisting of at least one representative from each of ITS, the data owner (e.g., OEM, Human Resources, Housing), and University Communications to prepare public announcements throughout the incident. In consultation with ITS, UPD and others, create a categorization and hierarchy of information with regard to its appropriateness for release, sensitivity, and criticality for dissemination. Public announcements and releases should include the following:

   - General what, when, where, who is affected, how, and, if possible, why.
   - What data is lost (non-recoverable).
   - What action impacted parties should take (e.g., contacting their financial institutions if their financial information or social security number was compromised).
   - What is the current status of compromised system.
   - What actions Humboldt will take to mitigate any exposure to harm to those affected by the compromise of the data.
   - Other appropriate questions and concerns.

4. Obtain permission of the Executive Committee and, if so directed by the Executive Committee, the Chancellor's Office to release the information.

5. Release the information via appropriate channels to the appropriate bodies.

   - Personal contacts by either ITS or the data owner if the number of impacted individuals is limited.
   - General public announcements (including to targeted constituencies), coordinated by University Communications. These might include bulk e-mail with reference to Web page and FAQ, link on campus homepage, press release to local media and/or a public forum.

6. Perform follow-up to review users' needs and analyze internal department practices.

Appendix A

Management Recovery Team

Emergency Team Coordinator - ITS **(ETC-ITS)**

Bill Cannon, Director, ITS

Office: (707) 826-3815

wcc7001@humboldt.edu

Backup Emergency Team Coordinator: **(BETC)**

Cliff Schall, Manager, TNS

Office: (707) 826-6114

cs1@humboldt.edu

2nd Backup Emergency Team Coordinator: **(2BETC)**

Nick DeRuyter, Interim Manager, UCS

Office: (707) 826-6164

njd2@humboldt.edu

Assistant to the Emergency Team Coordinator - ITS: **(AETC-ITS)**

Heather Tierney, Information Security Coordinator, ITS

Office: (707) 826-6117

security@humboldt.edu

The following managers are Alternates to the Emergency Team Coordinators for the Management Recovery Team. If none of the above-named ETCs are available following a disaster, the alternate listed below who arrives on campus first will be the ETC-ITS.

R.J. Wilson, Manager, Academic Computing

Office: (707) 826-4201

rjw7001@humboldt.edu

Steve Newman, Manager, Instructional Media Services

Office: (707) 826-3323

smn2@humboldt.edu

The following identifies the Emergency Team Coordinator and Backup for University Computing Services:

Emergency Team Coordinator - University Computing Services: **(ETC-UCS)**

Nick DeRuyter, Interim Manager, UCS

Office: (707) 826-6164

njd2@humboldt.edu

Backup Emergency Team Coordinator - UCS: **(BETC-UCS)**

Alan Lutje, Analyst, UCS

Office: (707) 826-6151

lutje@humboldt.edu

The following identifies the Emergency Team Coordinator and Backup for Telecommunications & Network Services:

Emergency Team Coordinator - Telecommunications & Network Services: **(ETC-TNS)**

Cliff Schall, Manager, TNS

Office: (707) 826-6114

cs1@humboldt.edu

Backup Emergency Team Coordinator - TNS: **(BETC-TNS)**

Jane Hansen, Operations Manager, TNS

Office: (707) 826-6131

hansenj@humboldt.edu

Appendix B

Disaster Recovery Teams

The following identifies the current staff for each Disaster Recovery Team including their contact numbers. Each Team member's role is consistent with his/her current job position. Duties assigned to each team are defined in Responsibilities of the Disaster Recovery Teams, Page 41.

Systems Recovery Team

Operations – Off-site Storage:

	Position	Office
Carol Morse	Operations Spec	x6127
Heather Tierney	Info Tech Consult	x6117

Sonoma State Univ. Offsite Storage: 1801 E. Cotati Avenue
Rohnert Park, CA 94928

Systems Recovery Team (continued)

Operating Systems:

	Position	Office
Mike Bradley	Sys Analyst/NT Admin	x6120
Bugs Brouillard	Unix Sys Admin	x6123
Nick DeRuyter	Sys Analyst/Unix Admin	x6164
Cliff Pratt	Unix Sys Admin	x6113

Hardware/Software Support:

Sandy Camozzi	ITC-ITS Webmaster	x6104
Barb Dyer	Info Tech Consult	x6110
Donna Smith	ITC- ITS Webmaster	x6152
Diane Sudori	Info Tech Consult	x6112

Technical Support Team – Banner/Oracle/FRS

	Position	Office
Mike Bradley	Sys Analyst	x6120
Nick DeRuyter	Sys Analyst	x6164
Peter Johnson	DBA	x6122
Alan Lutje	Sys Analyst	x6151
Ken Thrift	DBA/Sys Analyst	x6119
Liz Villarreal	Sys Analyst	x6159

User Liaison Team – Help Desk

	Position	Office
Central Number		x4357
Dan Cleaves	Help Desk Coord.	x6106
Melinda Christensen	Help Desk Asst.	x6251
Molly Simpson	Admin. Support Asst. II	x3815

Telecommunications & Network Services Team

	Position	Office
Central Number		x5000
Cliff Schall	Manager	x6114
Dave Budde	Equipment Spec	x6115
Vannat Chiem	Inst Support Asst II	x6184
Ben Curran	Network Analyst	x6130
Rick Garcia	Network Analyst	x6137
Jane Hansen	Operations Mgr	x6131
Shawn Hassell	Programmer/Analyst	x6162
Lisa Lewis	University Operator	x6103
Ronn McFadden	Network Analyst	x6145
Gary Peters	Network Analyst	x6139

Appendix D

Rentsys Mobile Recovery Services
for
Humboldt State University

In the event of a disaster, if an alternate site is necessary for the continued operation of University Computing Services, Humboldt State University has signed a contract with Rentsys Recovery Services to provide us with a mobile cold site. To supplement this cold site with necessary equipment, we have added Recover-All service to our maintenance agreement with Hewlett-Packard. Recover-All will repair or replace equipment covered in the maintenance agreement that has been disabled or destroyed as a result of the disaster. It will also cover the costs of the mobile cold site up to pre-defined limits.

200 QUALITY CIRCLE
COLLEGE STATION, TX 77845
Tel: (800)955-5171
FAX: (979)595-2711

DISASTER DECLARATION TEL: (866)736-8732

Acquiring the best information technology solutions is critical to a company's success. Equally important is protecting Information Technology assets from the devastation caused when vital computer systems are brought to a halt! Rentsys Recovery recognizes this and through our Business Recovery Services Program, we provide *peace of mind* with an added measure of business protection.

Rentsys Recovery's Business Recovery Services include a full range of end-user services and equipment for the most common operating platforms. We help you sustain near-normal on-line operation of your business functions – and your bottom line – under extraordinary or unusual circumstances, all from a single source.

Rentsys Recovery Services utilizes a three-phase approach: Plan, Prevent, Recover

PLAN

Business Recovery Planning and Consulting
Rentsys Recovery Service's Business Recovery Planning and Consulting Services provide you with the capability to design, implement, and manage effective enterprise-wide recovery programs. Our capabilities span all facets of disaster recovery planning – from identifying a client's vital business processes and applications to determining financial impacts of disasters,

identifying potential risks with solutions for disaster prevention, and defining critical technology and resources during disaster situations.

PREVENT

Data Center Site Services
Rentsys Recovery Services offers a complete portfolio of Data Center Site Services to assess the current data center facility and make recommendations for preventing potential disasters from occurring. Utilizing experts in the data center design and construction field, Rentsys Recovery Services can design solutions that may save you millions in downtime and lost business. From consulting to complete design and construction management, our disaster prevention solutions provide the most cost-effective method of disaster recovery…avoiding one in the first place.

RECOVER

Business Recovery Centers
Strategically located throughout the country, our Business Recovery Centers provide the equipment, technical resources and office infrastructure necessary to facilitate a fast and effective recovery from a major interruption. Rentsys Recovery Services and IBM partner to provide highly skilled operations, technical and administrative personnel throughout the emergency duration – and additional multi-vendor equipment and resources can be shipped and installed at the Business Recovery Center as required.

Mobile Recovery Centers
When you need the hot-site to come to you, our Mobile Recovery Center (MRC) – a fully configured, self-contained expandable trailer - will be there within 24 to 48 hours to begin your recovery process. These pre-installed configurations assure availability, and pre-testing assures rapid setup for applications compatibility. The units are delivered with systems connected to on-board hubs ready to be connected to a wide range of communications options.

Each Mobile Recovery Center contains a workstation area that includes multi-vendor hardware and communications lines connecting up to 150 users to either a remote site, a temporary alternate site, or to the original Data Center. These links can be expanded allowing connection to a central office ***WAN,*** through Satellite and Microwave connections to landlines facilitating data connectivity.

Disaster Protection Program
Rentsys Recovery Service's Disaster Protection Program (DPP) - a supplemental casualty-based program – offers immediate protection against disaster with 24 x 7 emergency response. With DPP your covered equipment is repaired or replaced in 24 to 48 hours following accidental damage.

Additional benefits include free installation, alternate site assistance, on site customer engineers, and *reimbursement* of the extra expenses, such as "notification and usage fees", facility cleanup, overtime and travel expense due to the covered casualty loss.

Customer Transit Insurance
Rentsys Recovery Service's Customer Transit Insurance program covers your equipment shipments from transit through installation at your site, and provides immediate replacement of any equipment damaged during shipment.

Business Recovery Services Customer Benefits:
⇒ "Peace of Mind"
⇒ Save time – one call to one vendor
⇒ Cost effective – the most practical options to answer contingent needs and facilities
⇒ Guaranteed access to skilled and specialized recovery teams
⇒ Convenience – no investments in time or equipment required
⇒ Flexibility – custom designed solutions to meet your needs
⇒ Increased employee morale – reduces travel, minimizes disruptions

Rentsys Recovery solutions provide you peace of mind, compliance to audit/statutory requirements, and the ability to focus your resources where they are needed most – ***your business***

Mobile Cold Site Recovery Center

INTRODUCTION
The Mobile Cold Site Recovery Center service provides, on site, on demand, rapid delivery of a fully configured, self contained, 43-53 foot van with a minimum expansion area of 29' x 16' for use as an equipment and user work area, to recover from a disaster or casualty loss.

Mobile Cold Site Recovery Center services, in this data sheet, will be provided in accordance with the terms and conditions on the Rentsys Recovery Services Agreement.

DESCRIPTION OF SERVICES
A Mobile Recovery unit will be delivered to the agreed customer's location, as described, upon notification of a disaster and subject to site access availability, within 24-48 hours of receipt of the Disaster Notification.

Rentsys will provide a complete mobile computing environment based in a 43-53 foot mobile computer center unit with onboard generator, air conditioning and expansion unit to house up to 50 workstations. Additionally, Rentsys will provide the microwave equipment and communications CPU to remotely operate additional workstations at a temporary alternate site located up to one half mile from the Mobile Recovery Center site. Up to 100 remote client PCs are optionally available.

AVAILABILITY OF SERVICES
Services are available, subject to "Multiple Disaster", 24 hours a day, 365 days a year, for a maximum of 45 days following receipt of the Disaster Notification.

NOTIFICATION
The customer must notify Rentsys through the emergency telephone number provided, of its request to use the Services.

The customer must follow the telephone notice with written notification, which may be faxed, within twenty-four (24) hours to Rentsys Recovery Services.

CHARGES

a) Upon acceptance of this agreement, the customer shall pay Rentsys Recovery the subscription fee set forth on the Mobile Cold Site Recovery Center Exhibit. The monthly subscription fee for Humboldt State University is $300.

b) The customer agrees to pay the Disaster Notification Fee for each activation of the service. This fee is $4,000.

c) The customer will pay to Rentsys Recovery a Daily Utilization Fee for each day or part thereof in excess of the first ten (10) days that the service is provided to customer. After the first ten days, the utilization fee is $800 per day.

d) Mobile Recovery Center coverage is available for additional locations at a discount of 50% of the primary (largest) location covered by the agreement.

Customer is Responsible for:

a) The development, testing and implementation of all procedures to be adopted in the event of a disaster.

b) The security and protection of confidential information, the Mobile Recovery Center and the equipment contained within.

c) The results of application whether restored and run by Rentsys Recovery or by the Customer.

d) All necessary permits, consents, and permissions (i.e. landlord's consent, planning permission, etc.)

e) Ensuring that the location, operation and running of the Mobile Recovery Center does not contravene any law, rule or regulation.

f) To provide Rentsys staff, adequate access to the area in which the service is to be located and ensure adequate office accommodations and facilities for Rentsys to perform its obligations under this agreement, including access for maintenance.

g) To ensure that the Mobile Recovery Center is not connected with any customer-supplied items (including hardware, software and telecommunications) without Rentsys Recovery's prior written consent.

h) To ensure there is no relocation of the Mobile Recovery Center or modification of it in any way.

i) The administration of the system(s), including loading of all tapes, disks or files and establishing the operational procedures. Rentsys will provide startup operation as deemed appropriate by Rentsys.

MULTIPLE DISASTERS
"Multiple Disasters" may be experienced by any number of subscribers. Accordingly, in such instances, Rentsys reserves the right to substitute comparable equipment for the service.

Such substitute equipment will be of equal or greater functionality to that in the Mobile Recovery Unit.

CONFIDENTIALITY
Rentsys and the customer will each exercise the same standard of care to protect any proprietary or confidential data of the other disclosed during negotiation or performance or this agreement as each uses to protect their own proprietary or confidential data.

LIMITATIONS
a) Rentsys is not liable for the provisions of any services, hardware, or software other than that set forth in the schedule.

b) Rentsys shall not be liable for any failure or delays in meeting obligations under the Agreement and this Data Sheet which are due to causes beyond Rentsys Recovery's reasonable control.

c) Rentsys may suspend performance of its obligations herein, without further liability, as a result of conditions which Rentsys believes represent a safety or health hazard. The customer shall be responsible to ensure the safety of Rentsys staff while at the location and to observe OSHA regulations.

RECOVERY TESTING
The customer agrees to pay the then current charges for all Recovery Testing Time agreed to and schedules.

All testing will be done at the location where the Mobile Recovery Center is permanently stationed.

TERM
1. The term of this Agreement is three (3) years unless otherwise listed in the Exhibit. At the expiration of the Initial Term, this Agreement will be automatically renewed for successive one (1) year period(s), at Rentsys Recovery's then prevailing rates unless written notice of termination is given.

2. After the Initial Term, this service may be canceled by the customer or Rentsys, by sending a written notice to the other at least ninety (90) days prior to such cancellation. The mailing of notice will be sufficient proof of notice.

For further information call:

1-800-955-5171
Fax: 1-979-595-2711
Web Site: http://www.rentsys.com

Appendix F

Hewlett-Packard's Recover-All Services

Recover-All Service is an enhancement to HEWLETT-PACKARD's onsite service agreements and warranties. While an onsite agreement protects Customer's multivendor computer equipment against mechanical failure and malfunction, Recover-All Service extends the agreement to provide protection from a specified, wide range of natural and man-made disasters, accidents, and environmental hazards.

Recover-All provides additional services that extend beyond the product repair and replacement aspects of a recovery. Realizing that equipment replacement is only one of the expenses associated with a disaster, Recover-All offers an array of additional services intended to reimburse the customer for many disaster related costs.

- Reimburse up to $50,000 in Hot Site notification and usage fees
- Reimburse up to $50,000 in Data Center rebuilding
- Reimburse for water damage and cleanup costs
- Plus many more

Recover-All Includes:

Alternate Processing Site

When covered property is damaged or destroyed by a covered peril and the data center containing the property is rendered unsafe or inoperable, requiring the Customer to occupy an alternate processing site, Recover-All Service will provide reimbursement, up to pre-defined limits, for the disaster notification fee and hourly/daily usage fees at an alternate processing site.

Loss of Facility Access

If the Customer is denied access to their facility—either by order of a civil authority or the facility is damaged by a covered peril and cannot be used for its intended purpose—and that loss of access prevents Customer from utilizing covered systems, Recover-All Service will provide reimbursement, up to pre-defined limits, for the cost of obtaining, installing and using temporary-use equipment at an alternate processing site.

No Deductible

Recover-All Service applies no deductible when replacing equipment which was destroyed by a covered peril.

Appendix G
Contact List for Academic Computing

If an emergency or disaster affects computing operations in Van Matre Hall, the staff in Academic Computing can be called to provide assistance to University Computing Services.

AC Staff	Ext.	Office
Main Office	4205	GH 213/218B
R.J. Wilson	4201	GH 218C
John Adorador	4209	GH 218A
Mark Hendricks	6141	GH 213A
Kishore Jayaswal	4212	GH 213
Tim Kohberger	4207	GH 213C
Madeline Myers	4210 4287	GH 213 P & T105
Laurie Takao	4207	GH 213C
Kimberly Vincent	6141	GH 213
Rocky Waters	4208	GH 213C
Jeanne Wielgus	4206	GH 213A

Computer Labs
The following shows the locations and the telephone numbers of the Computer Labs. Phone numbers are also given for Computer Lab servers that are located in separate rooms from the Lab.

Room	Ext.	Room	Ext.
FH 202	7206	LIB 310	7212
GH 215	7202	NHW 244	7215
GH 218	6166	SCI A364	7203
HGH 105	7208	SH 1	7200
HGH 229	7201	SH 118	7262
JH 212	7204	SH 119	7252
LIB 121	7207		

Appendix H
Contact List for Instructional Media Services

If an emergency or disaster affects computing operations in Van Matre Hall, the staff in Instructional Media Services can be called to provide assistance to University Computing Services.

Instructional Media Services Staff	**Ext.**	**Office**
Steve Newman	3323	GH205
Philip Hooker	3177	GH221
Jeremy Ketelsen	3169	GH205
Michael Penney	4200	SH119A
Riley Quarles	3644	L315
Andrea Schwandt-Arbogast	3633	L315
Will Seltzer	3175	GH221
Jodie Slack	3168	GH221
Natalie Walston	4200	SH119A
Robert Webster	3167	GH221

Appendix I
Quick Reference Campus Telephone Numbers

	Phone	Location
Campus Information Line	x4636	
Campus Operator	x3011	
Academic Affairs	x3722	SH216
Academic Computing	x4205	GH213
Center Activities	x3357	UC S Lounge
Earthquake Information Hotline	x6020	
Enrollment Management	x4402	SH211
Extended Education	x3731	SBS211
Financial Aid	x4321	SBS231
Health Center	x3146	Health Center
Housing & Dining Services	x3451	JGC
Human Resources	x3626	SBS143
Instructional Media Services	x3166	GH221
Library Information Desk	x3418	Lib110
Plant Operations Emergency Calls Plant Operations Maintenance/Service	x5900 x4475	
Procurement & Risk Management	x3512	SBS413
Public Safety/UPD Public Safety Administrative Line	x3456 x4487	SBS101
ResNet - Drew Meyer	x5529	JGC
Student Affairs	x3361	NHE216
University Advancement: Community Relations	x5100	SH6

Appendix K

First Aid & Survival Guide

The following information can be found in the Pacific Bell Telephone Directory for Humboldt County and is intended for reference purposes only. This material is not to be used in lieu of seeking appropriate medical attention.

Rescue Breathing for Adults - Basic CPR

1. Put your hand on the victim's forehead. While holding the forehead back gently pinch the nose shut with your fingers.
2. To open the airway, put your other hand under the victim's jaw, and lift the chin until it points straight up.
3. Take a deep breath. Open your mouth wide. Place it over the victim's mouth. Blow air into the victim until you see the victim's chest rise.
4. Remove your mouth from the victim's. Turn your head to the side and watch the chest fall while listening for air escaping from the victim's mouth. Give another breath.
5. If you hear air escaping and see the chest fall, Rescue Breathing is working. Continue until help arrives.
6. Check the victim's pulse.
7. Repeat a single breath every 5 seconds. Wait for chest deflation after each breath.
8. If you don't hear air escaping, airway is blocked.
9. If airway is blocked or the victim vomits, turn the victim on his or her side and sweep the mouth clear of vomit or other obstructions using two of your fingers.

Bleeding: Wounds

The best way to control bleeding is with direct pressure over the site of the wound. **Do not attempt to apply a tourniquet yourself.** Always avoid skin contact with the victim's blood. Use several layers of material, if necessary.

a. Apply firm, steady direct pressure for 5 to 15 minutes. Most bleeding will stop within a few minutes.
b. If bleeding is from a foot, hand, leg or arm use gravity to help slow the flow of blood. If there are no broken bones, elevate the limb so that it is above the victim's heart.
c. Severe nose bleeding can often be controlled by applying direct pressure by pinching the nostrils with the fingers while sitting up. Apply pressure 10 minutes without interruption.

Bleeding: Head Injuries

If there is bleeding from an ear, it can mean that there is a skull fracture.

1. Call for emergency help. Let a professional medical person attend the wound.
2. Always suspect a neck injury when there is a serious head injury. Keep the neck and head still.
3. Keep the airway open.
4. When stopping the bleeding, don't press too hard. **Do not attempt to stop bleeding from within the ear by direct pressure.**
5. **DO NOT** give the victim any fluids, cigarettes or other drugs. They may mask important symptoms.

Bleeding: Internal

Warning Signs:

a. Coughing or vomiting blood or passing blood in urine or stool.

b. Cold, clammy, pale skin; rapid, weak pulse; dizziness.

1. Get emergency medical help immediately.
2. Have the victim lie down with feet slightly elevated and relax. Stay calm and keep the victim warm.

Broken Bones

1. Call for emergency help or get someone to call for emergency medical help immediately.
2. **DO NOT** move the victim unless the victim is in immediate danger of further injury.
3. **DO NOT** try to push the broken bone back into place if it is sticking out of the skin.
4. **DO NOT** try to straighten out a fracture. Let a doctor or trained person do that. If you must move or transport the victim, immobilize or stabilize the fracture as best as possible.
5. Keep the victim warm, elevate the legs 6 to 12 inches and give no fluids or stimulants. Do not elevate the legs if you suspect an injury of the legs, neck, back or head.

Burns

1. Fire Burns

For small burns:

Cool the burn with running water to stop the burning process. Do not apply uncovered ice directly to the burn. If available, apply aloe vera to the burn. If ice is used, make sure it is contained in a bag or cloth.

For large burns:

Call 9-1-1. Make sure the burning has stopped, cover the victim with a dry, clean sheet.

2. Chemical Burns

- Remove victim's affected clothing.
- Wash burned areas with cool water for at least 20 minutes.
- Call 9-1-1 immediately.

For chemical burns of the eye: Flush eye with tepid water for 20-30 minutes.