

Table of Contents

Sections:

- I. Introduction and Purpose**
- II. Examples of Disasters and Risks**
- III. Initiate Emergency Procedures**
- IV. Assessment Procedures**
- V. Recovery Team**
- VI. Recovery Procedures**
 - a. Location**
 - b. Equipment**
- VII. External Business Partners**
- VIII. Disaster Recovery Plan Training and Testing**

I. Introduction and Purpose

This document is the emergency response plan for the University of Tennessee at Martin Information Technology Services. The information presented in this plan is a guide for University management and technical staff in the recovery of computing and communication facilities infrastructure and critical business applications. A full Business Continuity Assessment and Plan for the entire campus should be conducted to determine the risks, impact, and time (RTO-recovery time objective) that an office can operate without access to their electronic information. This plan does not address these issues. This plan attempts to set priorities for restoring services based on internal knowledge.

The ability to recover quickly from a small or large disaster is directly related to the amount of damage, and the time, money, and effort prior to the disaster that has been allocated to the redundancy of systems.

Currently every business operation of the campus is heavily dependent on electronic access to information and online communication. This change to technology dependency has taken place very quickly and continues to change each year.

Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup tapes. Data loss can occur between the point of the last backup and the time of the disaster. *Significant* effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point of the disaster forward.

Individual campus departments are responsible for developing their own procedures for operating until computer systems and communications networks can be restored and for managing the synchronization of their manual and restored data. The scope of this plan at this time does not address the needs of the off-campus centers in Selmer, Jackson, Ripley, and Parsons.

Consider the business impact of a disaster that prevents the use of the system to process Student Registration, Fee Payment, access to IRIS, or any other vital application for weeks. Students and faculty rely on our systems for instruction, all of which are important to the well-being of the University. Most people are lost without email, if they don't have access for a few hours. It is hard to estimate the damage to the University that such an event might cause. One tornado properly placed could easily cause enough damage to disrupt these and other vital functions of the University. Without adequate planning and preparation to deal with such an event, the University's central servers could be unavailable for many weeks.

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

A revised public version of this plan is available to the public on the UT Martin web site. (<http://www.utm.edu/its/>).

Primary OBJECTIVES of the Plan

This disaster recovery plan has the following primary objectives:

1. Add additional detail to the University of Tennessee at Martin Emergency Response Plan that is specific to technology and communications.
2. Present an orderly set of procedures for restoring critical communications systems within a currently undetermined amount of time.
3. Present an orderly set of procedures for restoring critical computer systems within a currently undetermined amount of time.
4. Identify human and physical resources needed for recovery.
5. Describe an organizational structure for carrying out the plan.
6. Plan future changes to make the infrastructure easier to recovery after a disaster

II. Examples of Disasters and Risks

FIRE

The threat of fire in the Crisp Hall server room area is real. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. There is a continuing problem with raccoons in the ceiling each spring and fall. The computers within the facility also pose a quick target for arson from anyone wishing to disrupt University operations. The fire suppression system is aging and in need of replacement.

FLOOD

The threat of a flood to Crisp Hall is not an issue. Improper drainage allowing water to penetrate the server room floor, which contains a significant amount of wiring, has been an issue in the past. At this point in time this has been resolved.

TORNADOS AND HIGH WINDS

Now that UT Martin is situated along the new "Tornado Alley", damage due to high winds or an actual tornado is a very real possibility. A tornado has the potential for causing the most destructive disaster we face. If the integrity of the Crisp Hall roof is compromised in the server room area, significant damage can occur.

EARTHQUAKE

The threat of an earthquake in the Martin area in the future is high. An earthquake has the potential for being the most disruptive for this disaster recovery plan because of the possibility of wide spread destruction. Restoration of computer systems and communications networks following an earthquake could be very difficult and require an extended period of time.

COMPUTER CRIME

Computer crime is a continuing threat that expands as systems become more complex and access is more distributed across the Internet.

III. Initiate Emergency Procedures

Initial Information Technology Services Notification Team

Name	Title
Helpdesk	881-7900
Shannon Burgin	Chief Information Officer
Will Turner	Security Administrator
Mark McAlpin	Manager Networking & Telecommunications
Terry Lewis	Director Security Server Administration Video Network
Brenda Wright	Director Operations Banner myUTMartin
Steve Holt	Director Web Services Instructional Technology
Susie Nanney	Director Digital Printing Services Computer Store
Tammy Overby	Business Manager
Karl Johnson	Manager Technical Services Field Support
Angela Fortner	Manager Helpdesk

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

Additional Contacts:

Banner

Larry Holder

Amy Belew

Don Parr

Doug Bloodworth

Network/Cable TV

Coy Hazlewood

Rick Gonzalez

Field Services /Copiers

Alan Franklin

Telephone

Roger Elmore

System Administration

Ken Blankenship

Bruce Harrison

Distance Learning

Bob Moseley

Nathan Tolene

CBORD/Filemaker

Steve Lemond

Web Site

Craig Ingram

Josh Kugler

UTC-Alternate Website

Monty Wilson

Secure all Information Technology Services locations

1. Computer Store
2. Digital Printing Services
3. Labs
4. Classrooms
5. Server room
6. Wiring Closets
7. Helpdesk call center
8. Helpdesk field support
9. Telecommunications room
10. Information Technology Services staff offices

Protect all backup media

Information Technology Services should have large plastic sheeting available in the server room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed to prevent water and wind damage. Operators should be trained how to properly cover the equipment.

In almost any disaster situation, hazards and dangers can abound. All personnel must exercise extreme caution to ensure that physical injury or death is avoided while working in and around the disaster site itself. No one is to perform any hazardous tasks without first taking appropriate safety measures.

Prepare Emergency Communications:

Switch to alternative emergency blogspot web site. Utilize the aircard if the network is unavailable and cell is available. As a last resort contact Knoxville or Chattanooga to help maintain the emergency web site.

www.utmemergency.com

Implement emergency alternative email addresses.

Consider the use of Facebook UTM Emergency Group for additional communications beyond those described early in this document.

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

Prepare the EOC Facilities:

Prepare the EOC (Crisp Hall Presentation Room) for communications. The cabinet in the Presentation Room contains the emergency communication supplies.

Bud Grimes and University Relations will be in the Public Safety Conference Room. Steve Holt's area will support Bud.

Information Technology Services will be in the Crisp Hall Conference Room.

The Helpdesk will be in the Online Configuration Room.

Determine Personnel Status

One of the important early duties is to determine the status of personnel working at the time of the disaster. Safety personnel on site after the disaster will effect any rescues or first aid necessary to people caught in the disaster. The list of the able-bodied people who will be available to aid in the recovery process should be identified by the Business Manager.

Taking care of our people is a very important task and should receive the highest priority immediately following the disaster. While we will have a huge technical task of restoring computer and network operations ahead of us, we can't lose sight of the human needs.

General Guidelines:

- Establish emergency communications based on what is not damaged
 - www.utm.edu and www.utmemergency.com
 - MyUTMartin and Blackboard
 - Mass email to campus-l
 - Hosted email services for critical accounts, if necessary
 - Autodialer to all campus phones
 - Banner TXT message to those who opt-in
 - Cable TV accessible channels
 - Helpdesk to receive phone calls
 - Ham radios
- Survey situation
 - Conduct site survey
 - Determine extent of damage
 - Salvage usable equipment
- Reestablish services

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

- Order necessary equipment
- Establish LAN connectivity
- Establish critical service

IV. Assessment Procedures

Damage Assessment Team

The Damage Assessment Team will be led by the Chief Information Officer, Security Administrator, and the IT Leadership Team. Other team members will include someone from each of the Director areas and the Physical Plant. This team will not be responsible for a detailed damage assessment for insurance purposes. The primary thrust for this team is to do two things:

1. Provide information to be able to make the choice of the recovery site.
2. Provide an assessment of the salvage ability of major hardware and network components.

Based on this assessment the recovery teams can begin the process of acquiring replacement equipment for the recovery.

V. Recovery Team

In a disaster it must be remembered that PEOPLE are your most valuable resource. The recovery personnel working to restore the communication and computer systems may be working at great personal sacrifice, especially in the early hours and days following the disaster. They may have injuries hampering their physical abilities. The loss or injury of a loved one or coworker may affect their emotional ability. They will have physical needs for food, shelter, and sleep. The University must take special pains to ensure that the recovery workers are provided with resources to meet their physical and emotional needs.

The Disaster Recovery Teams are:

1. Network and Telephone Recovery Team
2. Server Infrastructure Recovery Team
3. Applications Recovery Team
4. Equipment acquisition Team
5. Communications and Administrative Support Team

Plan of action:

1. Review damage assessment.
2. Check supplies, equipment, and tools available in the disaster recovery cabinet.
3. Determine which hardware, software, and supplies will be needed to start the restoration of a particular system.
4. Communicate list of components to be purchased and their specifications.
5. Review the recovery steps documented in this plan and make any changes necessary to fit the situations present at the moment.
6. When hardware begins to arrive, work with vendor representatives to install the equipment.

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

7. When all components are assembled, begin the steps to restore the operating system(s) and other data from the off-site backup tapes.
8. Attempt to recreate status of all systems up to the point of the disaster if possible.

VI. Recovery Procedures

Establish Location

If the central server room is destroyed in a disaster, repair or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer systems and communications services at an alternate site. The alternative cold site may be on campus in another building, somewhere within 25 miles, across the state at UTK or UTC. A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired. There are varying degrees of "coldness", ranging from an unfinished basement all the way to space where the necessary raised flooring, electrical hookups, and cooling capacity have already been installed, just waiting for the computers to arrive.

Other Options:

Hot Site

This is probably the most expensive option for being prepared for a disaster. A separate computer facility, possibly even located in a different city, can be built, complete with computers and other facilities ready to cut in on a moment's notice in the event the primary facility goes offline. The two facilities must be joined by high speed communications lines so that users at the primary campus can continue to access the computers from their offices and classrooms.

Disaster Recovery Company

A number of companies provide disaster recovery services on a subscription basis. For an annual fee you have the right to a variety of computer and other recovery services on extremely short notice in the event of a disaster. These services may reside at a centralized hot site or sites that the company operates, but it is necessary for you to pack up your backup tapes and physically relocate personnel to restore operations at the company's site. Some companies have mobile services which move the equipment to your site in specially prepared vans. These vans usually contain all of the necessary computer and networking gear already installed, with motor generators for power, ready to go into service almost immediately after arrival at your site. (**Note:** Most disaster recovery companies that provide these types of subscription services contractually obligate themselves to their customers to not provide the services to any organization who has not subscribed, so looking to one of these companies

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

for assistance after a disaster strikes will likely be a waste of time.)

Acquire Equipment

- Servers for
 - Domain controllers
 - Directory services
 - Filemaker tracking systems
 - Web services
 - Email services
 - Banner student services
 - myUTMartin portal
 - Xtender imaging
 - Touchnet payments
 - CBORD
 - Telephone system
 - Keyboards, monitors
 - Switches
 - Telephone switch
 - Air conditioning
 - Electrical power
 - Racks
 - UPS and generator
 - Network - Wiring/wireless
 - Voice
 - Video
 - Data
 - Switches
 - Routers
 - VPN's
 - Other network appliances
 - Laptops for individual use
 - Multifunction Devices
 - Desks, chairs, tables
 - Telephones
 - Security
- Prepare the recovery location
- Locate usable backups for recovery
- Order, install, and configure a network
 - Establish voice communications
 - Establish LAN

UT Martin Information Technology Services
Emergency Response Plan - WORKING Active Document

- Establish WAN connectivity
- Order, install, connect, and restore information to the servers from backups
- Follow individual recovery plans for each system

The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configuration. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. The Recovery Management Team will have the expertise and resources to work through these problems as they are recognized. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

VII. External Business Partners

NEC – Telephone System (contact through Roger Elmore)

Dell, Gateway, Apple – Servers and laptops (contact through Susie Nanney)

Xiotech/Howard – storage (contact through Susie Nanney)

HP – network (contact through Susie Nanney)

Dell – Banner Student Services (contact through Susie Nanney)

SungardHE – Banner software, Xtender Software, Touchnet software (contact through Larry Holder)

Microsoft – server software, email (contact through Susie Nanney)

CBORD, Basis, Stanley – lock systems and card access (contact through Steve Lemond)

Blackbox – network (contact through Mark McAlpin)

Qwest, Charter, Frontier, Greenlight – network – (contract through Mark McAlpin)

Blackboard – course management system (contract through Bruce Harrison)

VIII. Disaster Recovery Plan Training and Testing

1. Review and change this plan on a yearly basis
2. Review and change detailed system, network, and application plans on a yearly basis