Table of Contents

Sections:

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 any of the off-campus centers.

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 systems could be unavailable for many weeks.

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 recover 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. A new automatic whole room inert gas based fire detection and suppression system was installed into the machine room, network room, and telecom switch room in the summer of 2011.

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. The US Geological Survey rates the nearby New Madrid Fault as perennially imminent for a major earthquake. 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.

PANDEMIC SICKNESS OUTBREAK
With the arrival of new viruses and illnesses, a plan to continue operations in the event of a pandemic outbreak is needed. If the illness spreads through the UT Martin campus, it is expected that the campus will be closed to prevent additional cases. All essential IT functions will need to remain active and in full working order to allow classes to continue in an online venue.

III. Initiate Emergency Procedures

Initial Information Technology Services Notification Team

Name	Title	Contact Information
Helpdesk		731-881-7900
Terrance Phifer	Helpdesk IT Technologist III	
Craig Ingram	Helpdesk Web Services Instructional Technology	
Terry Lewis	Chief Information Officer	
Brian Stubblefield	Security Administrator	
Mark McAlpin	Manager Networking & Telecommunications	
Amy Belew	Director, Security Server Administration Video Network	
Amy Belew	Director Operations Banner myUTMartin	
Susie Nanney	Director Digital Printing Services Computer Store (Finance & Administration)	
Tammy Overby	Business Manager	
Alan Franklin	Manager Technical Services Field Support	

Additional Contacts:

Banner	Larry Holder Brenda Wright Doug Bloodworth Amy Belew
Portal	Steven Robertson
Xtender	Steven Robertson
Touchnet	Doug Bloodworth
Network/Cable TV	Will Turner Mark McAlpin
Field Services /Copiers	Alan Franklin Scott O'Neal
Telephone	Roger Elmore
System Administration	Corey Jones Bruce Harrison
Distance Learning	Bob Moseley Nathan Tolene
CBORD	Steve Lemond
Web Site	Craig Ingram Weston Gentry
UTC-Alternate Website	Tom Hoover

Secure all Information Technology Services locations

1. Computer Store (Finance & Administration)
2. Digital Printing Services (Finance & Administration)
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 and in the means of shutting down electrical power to the machine room.

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 Verizon MiFi device if the network is unavailable and cell is available. As a last resort contact Knoxville or Chattanooga to help maintain the emergency web site.

Implement emergency alternative email addresses.

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

Prepare the EOC Facilities:

Prepare the EOC (Technical Support Service office area, formerly the Crisp Hall Presentation Room) for communications. The cabinet in the Research and Development Area contains the emergency communication supplies.

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

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

The Helpdesk will be in the R&D 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 affect 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 Information list
    - Hosted email services for critical accounts, if necessary
    - Utilize Zoom for video conferencing
    - Autodialer to all campus phones
    - RAVE Wireless opt-in text messaging
    - 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
    - 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.
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

The University of Tennessee at Martin, Office of Information Technology Services, currently operates a beginning stage disaster recovery site located at UT Chattanooga. This location currently houses a secondary Tegile Storage Area Network (SAN). The identical Tegile SAN is located on the UT Martin campus, which holds all of the datastores for our VMWare virtual server environment as well as all high profile data including our Banner Information Systems database, replicates data to the secondary SAN in Chattanooga. In the event of a disaster which rendered the computer center on the UT Martin campus unusable, the UT Chattanooga site will still have a backup of the critical data. In a total loss scenario, as currently implemented, a full rebuild of the physical server and network infrastructure will be required either in a new location or possibly at the UT Chattanooga site and then hook into the Tegile SAN at that site.

The current implementation of a disaster recovery site is primarily an off-site data backup. As funding becomes available, the preference would be to procure the server and network infrastructure required to implement a full hot disaster recovery site.

Acquire Equipment

- Additional servers for VMWare hosts
  - Domain controllers
  - Directory services
  - Filemaker tracking systems
  - Web services
  - Email services
  - Banner student services
  - myUTMartin portal
  - Xtender imaging
  - Citrix virtualization
  - CBORD
  - Telephone system
  - KMS
  - UTM Certificate Server
  - Public Safety Server
  - Student Health Server
  - Vcenter Server
- 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
    - 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. Pandemic Viral Outbreak

In the event that the campus experiences an extensive viral outbreak, certain steps must be taken to help prevent the spread of disease among the UT Martin community.

Computer Labs

If a moderate flu outbreak is declared which necessitates the suspense of campus gatherings of 100 people or more, all computer labs will be shut down. Computer keyboards, mice and tables are surfaces which could easily be contaminated and transmit flu virus. The following protocols will be followed to help prevent the spread of the virus:

- All lab computers will be shut down and their input devices removed.
- Students will be notified of the computer lab closures through the MyUTMartin portal.
- Faculty will be notified of the computer lab closures through the Information email list.

Campus closure

If a severe flu outbreak is declared and the campus is closed, the following measures will be implemented to assist the campus administration in communicating with the UTM community and to support the continuation of classes in a distance learning environment.

- Necessary emergency alert measures will be activated to facilitate enhanced communications.
- The IT Leadership team will assess the current resources and needs to include the availability of IT staff to work on-site or remotely and determine alternate personnel to fill gaps in IT staffing during illness.
- Most IT staff are expected to telecommute during the campus closure. Only necessary, designated personnel are to be present on campus during the closure.
- All systems are expected to remain up and active during the campus closure. All system upgrades will be suspended.
- Network traffic will be closely monitored and traffic shaping will be adjusted to ensure that essential mission critical traffic types are given bandwidth priority.
- The helpdesk will remain open and be prepared to field questions surrounding distance learning, video conference, Blackboard, and other systems used to hold classes during campus closure. Full time help desk analysts will be fielding calls from home or from individual offices to reduce contact with others that could spread the flu virus.
- Access to administrative systems will be available to staff through VPN connectivity.

- ITC Personnel will remain available to assist Faculty in establishing remote courses using Blackboard, Adobe Connect and Adobe Presenter, and other technologies.
- The following online resources will be utilized and/or maintained to facilitate online courses during the campus closure:
  - Blackboard
  - Zoom
  - Streaming server
  - WUTM Radio and streaming
  - Echo 360 (11 rooms)
  - Videoconferencing H.323 (8 rooms)
  - Webcasting
  - Google Apps
  - iTunes U
  - YouTube
  - Email
  - Teleconferencing

VIII. External Business Partners

NEC – Telephone System (contact through Roger Elmore)

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

PCS – Tegile storage (contact through Susie Nanney)

HP – network (contact through Susie Nanney)

Dell – Banner Student Services (contact through Susie Nanney)

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

Touchnet – PCI (contact through Doug Bloodworth)

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

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

INC – network (contact through Mark McAlpin)

AT&T, Charter, Frontier, Greenlight, Weakley County Municipal Electric Service – network – (contract through Mark McAlpin)

Blackboard – course management system (contract through Bruce Harrison)

Citrix/PCS – Knoxville, TN (contact through Susie Nanney)

Planet Technology – Microsoft Exchange and Microsoft Lync (contact through Susie Nanney)

Barracuda/IT Select – load balancers (contact through Susie Nanney)

NDM Technologies – SIEM and Firewall (contact through Susie Nanney)

Compview – Extron Classroom Technology (contact through Susie Nanney)

CCS – Epson Projectors and document cameras (contact through Susie Nanney)

Layer 3 – Wireless Network Equipment (contact through Susie Nanney)

IX. 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 or when major changes occur
3) Training occurs as needed and as roles or responsibilities are update