THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT0128-M - Contingency Planning	
Version: 3	Effective Date: 10/12/2022

Objectives:

To establish a formal, documented plan for managing the risk of information asset failures and service disruptions through the establishment of an effective contingency planning program.

The primary objectives of this plan are:

- Present a set of procedures for restoring critical communications and computer systems,
- Identify human and physical resources needed for recovery,
- Describe an organizational structure for carrying out the plan, and
- Add additional detail to the University of Tennessee at Martin Emergency Response Plan that is specific to information technology and communications.

Scope:

This plan applies to all users of, and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its regional centers.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this policy is based on those guidelines. This plan is based on guidelines in *NIST Special Publication 800-34 Revision 1 Contingency Planning Guide for Federal Information Systems.*

UTM must develop or adopt and adhere to a plan that demonstrates compliance with related policies and standards.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of University policy is assumed if a User accesses, uses, or handles University resources.

Plan Details:

This document also serves as 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 for recovering computing and communication facilities, infrastructure, and critical business applications. This plan attempts to set priorities for restoring services based on internal knowledge.

Data recovery efforts in this plan are targeted at getting the systems up and running with the latest backups or replications. Data loss can occur between the point of the last backup or replication and the time of the disaster.

The scope of this plan currently does not address the needs of the regional centers.

Roles and Responsibilities:

Chief Information Officer: Has overall accountability for contingency planning as the Position of Authority.

Director of IT Infrastructure: Responsible for overseeing the implementation, maintenance, testing, and execution of contingency planning activities.

Individual campus departments: Responsible for developing procedures for operating until computer systems and communications networks can be restored, and for managing the synchronization of their manual and restored data.

Disaster Recovery (DR) Site Overview:

The University of Tennessee at Martin Office of Information Technology Services currently operates a DR site located at another campus in the UT system. This location currently houses a secondary Storage Area Network (SAN) and compute resources. The primary SAN is located on the UT Martin campus and holds all the datastores for the VMware virtual server environment and replicates data to the secondary SAN regularly (CP-6). In the event of a disaster which renders the data center on the UT Martin campus unusable, the DR site will have a replica of the critical data. In a total loss scenario, as currently implemented, a full restoration of the virtual infrastructure will be performed at the DR site.

Examples of Disasters and Threats:

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. The computers within the facility also pose a quick target for arson from anyone wishing to disrupt University operations. Automatic inert gas-based fire suppression systems are installed in the datacenter, network room, and telecom switch room. The remainder of the wood-construction building has no fire protection.

Tornadoes and High Winds
Due to the increase in tornado activity in the region, the threat of damage due to a tornado or high winds is growing. A tornado has the potential to be one of the most destructive disaster we face.

Earthquake
The threat of an earthquake in the Martin area is high. The New Madrid Seismic Zone is the most active seismic area in the US east of the Rocky Mountains. An earthquake has the potential for being the most disruptive for this disaster recovery plan because of the possibility of widespread destruction.

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

Viral Outbreak
If an 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 available to allow classes to continue in an online venue.

Contingency Plan:

Specific procedures for recovery activities are contained in related documents IT0128-M-C through IT0128-M-E (CP-1).

Secure all Information Technology Services Locations

- Labs
- Classrooms
- Server room
- Wiring Closets
- Help Desk call center
- Help Desk field services
- Telecommunications room
- Information Technology Services staff offices

Protect Equipment

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.

All personnel must exercise extreme caution 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 blogger.com emergency website.
- Utilize Verizon MiFi devices if the campus network is unavailable and cell service is available.
- As a last resort, contact Knoxville or Chattanooga to help maintain the emergency web site.

Prepare the EOC Facilities

- Prepare the EOC for communications:
    - Chancellor’s Conference Room, Hall Moody Administration Building (primary location)
        - Public Safety Conference Room, Crisp Hall (alternate location)
        - Maintenance Center Conference Room (alternate location)
    - University Relations will be in the Public Safety Conference Room.
        - Web Services will support University Relations.
    - Information Technology Services will be in the Crisp Hall Conference Room.
    - The Help Desk will remain in the current location in Crisp.

Determine Personnel Status

One of the important early duties is to determine the status of personnel at the time of 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.

See *IT0128-M-A - Contact Information* for ITS employee contact information.

General Guidelines

- Establish emergency communications based on what is not damaged
    - www.utm.edu
    - MyUTMartin Portal
    - Canvas
    - Mass email to Information list
    - Zoom and/or Teams
    - Autodialer to all campus phones
    - Rave Alert notifications
- Survey situation
    - Conduct site survey
    - Determine extent of damage
    - Salvage usable equipment
- Reestablish services
    - Activate DR site, if necessary
    - Establish LAN and WAN connectivity
    - Help Desk to receive phone calls
    - Order necessary equipment
    - Cable TV accessible channels

Assessment Procedures:

Damage Assessment Team

The Damage Assessment Team will be led by the Chief Information Officer, IT Leadership Team, and Security Administrator. 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 purpose for this team is to:

- Provide information to be able to make the choice of the recovery site; and
- Provide an assessment of the salvageability of major hardware and network components.

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

Disaster Recovery Teams

- Network and Telephone Recovery Team (Network Administrators, Technical Specialist, Telecommunications Manager)
- Server Infrastructure Recovery Team (System Administrators)
- Applications Recovery Team (Senior Database Administrator, System Analysts and Administrators)
- Equipment acquisition Team (Director of IT Infrastructure, Computer Store Manager)
- Communications and Administrative Support Team (Director of Web and Client Services, Business Manager)

Plan of Action

- Review damage assessment.
- Check supplies, equipment, and tools available in the disaster recovery cabinet.
- Determine which hardware, software, and supplies will be needed to start the restoration of a particular system.
- Communicate list of components to be purchased and their specifications.
- Review the recovery steps documented in this plan and make any changes necessary to fit the current situation.
- When hardware begins to arrive, work with vendor representatives to install the equipment.
- When all components are assembled, begin the steps to restore the operating system(s) and other data from the backups or replications from our disaster recovery site.
- Attempt to recreate status of all systems up to the point of the disaster if possible.

Recovery Procedures:

Acquire Equipment

See *ITS0128-M-B - External Business Partners* for external business partner contact information.

- Servers for VMWare hosts
- SAN
- Telephone system
- KVMs, keyboards, monitors, and mice
- Server racks
- Air conditioning
- Electrical power, UPS, generator
- Networking - Wiring, switches, routers, firewalls, wireless, load balancers, etc.
- Laptops for individual use
- Multifunction Devices and paper
- Desks, chairs, tables
- Telephones

Prepare the disaster recovery location

See *ITS0128-M-E - Disaster Recovery Site Procedures*.

Prepare usable backups or replications for recovery

Order, install, and configure a network

- Establish voice communications
- Establish LAN
- Establish WAN connectivity

See *IT-0128-M-F - Network DR Overview* for information regarding restoring fiber connectivity on campus.

Order, install, connect, and restore information to the servers from backups or replications

See *IT1028-M-D - Datacenter Cold Start Procedures* for guidance on starting up systems.

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 Disaster Recovery Teams 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.

Pandemic Outbreak:

In the event the country experiences an extensive viral outbreak, Centers for Disease Control (CDC) guidance will be followed to help prevent the spread of disease among the UT Martin community.

Computer Labs

If a viral outbreak is declared which necessitates the suspense of campus gatherings, all computer labs will be closed. The following protocols will be followed to help prevent the spread of the virus:

- All lab computers will be closed, and tables and input devices sanitized,
- Students will be notified of the computer lab closures through the MyUTMartin Portal, and
- Faculty will be notified of the computer lab closures through the Information email list.

Campus Closure

If the campus is closed by national or state mandate, 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, if necessary.
- IT staff are expected to telecommute during campus closure. Only essential service providers are required to be present on campus.
- All systems are expected to remain available.
- Network traffic will be closely monitored. Traffic shaping may be adjusted to ensure that essential mission critical traffic is given bandwidth priority.
- Available Help Desk staff will field calls remotely to reduce contact with others.
- ITC Personnel will remain available to assist faculty with online instruction.
- Specified lab computers will be made available via VPN to students who need access to certain applications for classes.

The following online resources will be utilized to facilitate online courses during the campus closure:

  - Canvas
  - Zoom
  - Microsoft 365
  - Google Apps
  - Application Streaming
  - Remote access to computer lab software

Contingency Plan Training:

Personnel training for disaster recovery should coincide with tests and exercises and occur as roles and/or responsibilities are updated (CP-3).

Contingency Plan Testing and Updating:

Regular tests and exercises for disaster recovery should be performed regularly (CP-4). Detailed system, network, and application plans should be reviewed regularly and updated as needed or when major changes occur (CP-2).

Information System Backups:

Servers are backed up using Veeam. Servers should be backed up daily and the restore points kept for at least 60 days (CP-9).

Information System Recovery and Reconstitution:

Servers can be restored using Veeam or SAN replication (CP-10).

Random VMs will be selected and recovered at least once a quarter for testing (CP-4).

Resilience Requirements for Business-Critical Servers:

Servers used for business-critical services should be run as a VM (Virtual Machine) in the VMware infrastructure. If standalone hardware must be used, the following options must be used to ensure maximum uptime:

- High-availability, failover clustering, load balancing, etc.
- Redundant power supplies connected to separate circuits
- Redundant NICs (Network Interface Card) connected to separate switches
- RAID (Redundant Array of Independent/Inexpensive Disks) storage
    - RAID level must utilize mirroring and/or distributed parity
- Data and/or configuration files must be backed up and/or replicated to the DR site
- Logging setup to the SIEM (Security Information and Event Management)

Exceptions:

Exceptions must be noted and presented to the IT Security Team for review if any of the resiliency requirements are not technically feasible.

References:

IT0128 - Contingency Planning

IT0128-M-A - Contact Information

IT0128-M-B - External Business Partners

IT0128-M-C - Datacenter Orderly Shutdown Procedures

IT0128-M-D - Datacenter Cold Start Procedures

IT0128-M-E - Disaster Recovery Site Procedures

IT0128-M-F - Network DR Overview

NIST SP 800-34 Revision 1 - Contingency Planning Guide for Federal Information Systems

NIST SP 800-53 Revision 5.1, Security and Privacy Controls for Information Systems and Organizations

Definitions:

Compute Resources: An object that represents a host, host cluster, or pool in a virtualization platform on which machines can be provisioned.

Disaster - Any hazard event that causes significant damage and/or loss of functionality.

Essential Service Provider - Personnel who engage in activity that directly supports critical services and/or infrastructure.

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation) or assets through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.