Disaster Recovery
and
Backup Data Plan

June 2020
Revised April 2021

TABLE OF CONTENTS

Section 1: Introduction

Faculty, staff and students of Mississippi Valley State University (MVSU) all rely heavily on the Department of Information Technology (IT) to accomplish their work and as an integral part of the learning environment.

Because of this reliance, IT is considered a critical component in the daily operations of Mississippi Valley State University, requiring a comprehensive Disaster Recovery Plan to assure that these services can be re-established quickly and completely in the event of a disaster of any magnitude.

Response to and recovery from a disaster at Mississippi Valley State University is managed by the university's Disaster Recovery Management Team. The Mississippi Valley State University Emergency Operations Plan governs their actions.

This IT Disaster Recovery Plan presents the requirements and the steps to take in response to and for the recovery from any disaster affecting IT services at Mississippi Valley State University, with the fundamental goal of allowing basic business functions to resume and continue until such time that all systems can be restored to pre-disaster functionality.

Mississippi Valley State University possesses a Unitrends 814S Appliance with 10TB of local disk space located at locally on campus in the main data center for quicker recovery of some operations. Also available are 2TB of cloud storage to backup critical servers and data.

Section 2: Scope

Due to the uncertainty regarding the magnitude of any potential disaster on the campus, this plan will only address the recovery of systems under the direct control of the Department of Information Technology that are critical for business continuity. This includes the following major areas:

- Authentication and network directory services
- On-premises enterprise applications (e.g. Banner, Nuvision, Booklog, and Evision Apps)
- Datacenter
- On-premises file shares and services
- Desktop equipment, labs, and classrooms
- Data networks and telecommunications (wired and wireless networks, telephony)

An increasing number of critical services are no longer hosted by the university, including systems crucial for daily activities. The recovery of these systems themselves is beyond the scope of this document and the ability of the IT department, but this plan will address restoration of connectivity and integration with these services. This includes the following major services:

- Learning management system (Canvas)
- Email (Office 365)
- Website (US Next)

This plan covers all phases of any IT related disaster occurring at Mississippi Valley State University. These phases include:

- Incident Response
- Assessment and Disaster Declaration
- Incident Planning and Recovery
- Post Incident Review

Section 3: Assumptions

This disaster response and recovery plan is based on the following assumptions:

Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in the IT Disaster Recovery Plan will be available.

The safety of students, staff, and faculty are of primary importance and the safeguard of such will supersede concerns specific to hardware, software and other recovery needs.

Depending on the severity of the disaster, other departments/divisions on campus may be required to modify their operations to accommodate any changes in system performance, computer availability and physical location until a full recovery has been completed. The Information Technology Department will encourage all other departments to have contingency plans and Business Continuity Plans for their operations, which include operating without IT systems for an extended period of time.

The content of this plan may be modified and substantial deviation may be required in the event of unusual or unforeseen circumstances. These circumstances are to be determined by the IT Director.

Section 4: Definitions

Backup/Recovery Files: Copies of all software and data located on the central servers, which are used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.

Catastrophic Disaster: A catastrophic disaster will be characterized by expected downtime of greater than 7 days. Damage to the system hardware, software, and/or operating environment requires total replacement / renovation of all impacted systems.

Datacenter Recovery: Individuals responsible for the establishment of an operational datacenter, either by returning the primary center to operational status or by bringing a cold site online for use.

Desktop, Lab, and Classroom Recovery Team: Individuals responsible for the recovery and testing of desktop computers and services, classrooms, and labs in the affected areas at Mississippi Valley State University.

Disaster Recovery Team: The DRT is a team of individuals with the knowledge and training to recover from a disaster.

Disaster: Any IT incident, which is determined to have potential impacts on the business continuity and ongoing operations of Mississippi Valley State University.

Crisis Management Team: The CMT is the first to respond to an incident, to secure and contain the situation. The CMT may consist of university personnel, firefighters, police, security, and other specialized individuals.

Equipment Configuration: A database (either soft or hard copy) which documents the configuration information necessary to return any IT hardware (server, network, desktop) to pre-disaster configurations. This includes hardware revisions, operating system revisions, and patch levels.

Incident Command Headquarters: Location where the ICTs meet and coordinate all activities with regard to assessment and recovery. For the IT Department, the headquarters is located at the Annex I Building.

Incident Command Team: The ICT is a group of IT individuals with combined knowledge and expertise in all aspects of the IT organization. It is the responsibility of the ICT to perform the initial assessment of the damage, to determine if a formal "disaster" declaration is required and to coordinate activities of the various IT DRTs.

Incident Commander (IC): The Incident Commander leads all efforts during the initial assessment of the incident, in conjunction with the Incident Command Team (ICT). If a disaster is declared, the IC is responsible for overall coordination of all IT related recovery activities. For Mississippi Valley State University, the Incident Commander is the Director of Information Technology.

Incident: Any non-routine event that has the potential of disrupting IT services to Mississippi Valley State University. An incident can be a fire, wind, storm, significant hardware failure, flood, virus, Trojan horse, etc.

Major Disaster: A major disaster will be characterized by an expected downtime of more than 48 hours but less than 7 days. A major disaster will normally have extensive damage to system hardware, software, networks, and/or operating environment.

Infrastructure and Web Recovery: Recovery and testing of infrastructure systems at Mississippi Valley State University including Active Directory, DNS, email, server virtualization, and web services. In the cases where these services are hosted off-premises, this team is responsible for re-establishing connectivity, authentication, and integration of those systems.

Minor Disaster: A minor disaster will be characterized by an expected downtime of no more than 48 hours, and minor damage to hardware, software, and/or operating environment from sources such as fire, water, chemical, sewer or power etc.

Enterprise Applications Recovery Team: Individuals responsible for the recovery and testing of Banner and other enterprise applications. For those systems hosted off-premises, such as Banner, this team is responsible for re-establishing connectivity, authentication, and integration of those systems.

Routine Incident: A routine incident is an IT situation/failure that is limited in scope and is able to be addressed and resolved by a specific team or individual as part of their normal daily operations and procedures.

Network and Telecommunications Recovery: Recovery and testing of data and voice networks.

Web Services: All services related to Mississippi Valley State University's Internet and intranet web activities and presence. The primary web service provided by the university is the homepage at www.mvsu.edu.

Section 5: Teams

5.0.1 Incident Commander

IT Director:
Office Phone: 662-254-3744
Cell Phone:

5.0.2 Incident Command Team

Assistant IT Director: Carmela Staten
Office Phone: 662-254-3649
Network Manager Steven Pitchford
Office Phone: 662-254-8401

5.1 Datacenter Recovery Team

All Contact Information is located in Appendix A

The Datacenter Recovery Team is composed of personnel within the Information Technology department that support the university's central computing environment and the primary datacenter where all central IT services, the Networks Operations Center (NOC) and other central computing resources are located. The primary function of this working group is the restoration of the existing datacenter. This team's role is to restore the datacenter to a condition where individual recovery teams can accomplish their responsibilities with regard to server installation and application restoration.

The team should be mobilized only in the event that a disaster occurs that impact the ability of the existing central computing facility to support the servers and applications running there.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of this recovery effort will normally be accomplished prior to most other recovery efforts on campus as having a central computing facility for the recovery of most applications and IT services to the campus.

5.2 Desktop, Lab, and Classroom Recovery Team

All Contact Information is located in Appendix A

Team Lead:	Sr. Computer Technician
Team Members:	Network Manager
	Network Technician
	Computer Technician

The Desktop, Lab, and Classroom Recovery Team is composed of personnel within the

Information Technology department that support desktop hardware, client applications, classrooms, and labs. The primary function of this working group is the restoration of MVSU's desktop systems, classrooms, and labs to usable condition. During the initial recovery effort, the team is not responsible for restoration of any data the user may have on their desktop computer. Mississippi Valley State University recommends all users store data files on the file servers, which are backed up nightly, to support data recovery.

The team should be mobilized in the event that a significant interruption in desktop, lab, or classroom services has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation. The IT Incident Commander will accomplish the coordination of this recovery effort with other recovery efforts on campus.

5.3 Enterprise Systems Recovery Team

All Contact Information is located in Appendix A

The Enterprise Systems Recovery Team is composed of personnel within the Information Technology department that support Banner and other enterprise systems. The primary function of this working group is the restoration of all modules of Banner applications to the most recent pre-disaster configuration in cases where data or operational loss is significant. In less severe circumstances, the team is responsible for restoring the system to functional status as necessitated by any hardware failures, network outages, or other circumstances that could result in diminished system operation or performance.

The team should be mobilized in the event that Banner or the other enterprise systems experience a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

This team will coordinate its activities and be responsible for hosting, managing, and supporting Banner and their respective Oracle databases.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation. The IT Incident Commander will accomplish the coordination of the enterprise systems recovery effort with other recovery efforts on campus.

Team Lead:	Assistant Director/Application Manager
Team Members:	Programmer
	Information Technology Specialist

5.4 Infrastructure and Web Recovery Team

All Contact Information is located in Appendix A

The Infrastructure and Web Recovery Team is composed of personnel within the Information Technology department that support the university's network infrastructure, including Active Directory, DHCP, DNS, email, file servers, network applications, network storage, server virtualization, and web services. The primary function of this working group is the restoration of the network infrastructure and servers to their most recent pre-disaster configuration in cases where data and operational loss is significant. In less severe circumstances, the team is responsible for restoring the system to an functional status as necessitated by any hardware failures or other circumstances that could result in diminished operation or performance.

The team should be mobilized in the event that any component of the network infrastructure experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

In the case of off-premises services, this team will coordinate restoration of these services with the external vendors or organizations responsible for providing them.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation. The IT Incident Commander will accomplish the coordination of this recovery effort with other recovery efforts on campus.

Team Lead:	Webmaster
Team Members:	Assistant Director
	IT Director

5.5 Telecommunications, Network, and Internet Services Recovery Team

All Contact Information is located in Appendix A

The Telecommunications, Network, and Internet Services Recovery Team is composed of Personnel within the Information Technology department that support the university's voice and data networks including cable plants, switches, and routers. The primary function of this working group is the restoration of our voice and data networks and Internet services to the most recent pre-disaster configuration in cases where operational loss is significant. In less severe circumstances, the team is responsible for restoring the voice and data networks and Internet services to an functional status as necessitated by any failures or other circumstances that could result in diminished operation or performance.

The team should be mobilized in the event that any component of the voice or data networks experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the IT Incident Commander up to date regarding the nature of the disaster and the steps being taken to address the situation. The IT Incident Commander will accomplish the coordination of this recovery effort with other recovery efforts on campus.

Team Lead:	Network Manager
Team Members:	Network Technician
	IT Director

5.6 Critical Mississippi Valley State University Contacts

A copy of the Mississippi Valley State University Emergency Response Contacts List is located in Appendix B

Section 6: Recovery Preparations

A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" as possible. Specifically, this section addresses the backup and storage practices as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

6.1 Data Recovery Information:

Backup/Recovery files are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. Backup job locations and retention periods summarized in the table below:

Type:	Location:
Daily Backup (disk)	Datacenter, Unitrends Appliance
Weekly Backup	Datacenter, Unitrends Appliance, Unitrends Cloud, Safety Deposit Box

Mississippi Valley State University does not have systems in place to backup and restore information/data located on individual desktop systems throughout the campus. Only the servers located in the datacenter are backed up; as such, only data resident on these systems will be able to be recovered. In the event that a disaster occurs on the campus that destroys personal computers, the information located on these computers will be extremely difficult or impossible

to recover. If recovery is possible, it will require outside vendor involvement at great expense to the user.

The Information Technology department recommends and encourages the use of USB storage devices and University Office 365 OneDrive accounts to store all important files. The recovery of data not backed up to a USB drive and/or OneDrive accounts are not covered under this plan.

6.2 Central Datacenter and Server Recovery Information:

In the event of any disaster, which disrupts the operations in the datacenter, reestablishing the datacenter will be the highest priority and a prerequisite for any IT recovery. As such, the Information Technology department is required to have detailed information and records on the configuration of the datacenter and all servers and ancillary equipment located in the datacenter. Detailed information is documented in our monitoring system and infrastructure website. The infrastructure staff is responsible for keeping the hardware inventory up to date.

6.3 Network and Telecommunication Recovery Information:

In the event of any disaster, which disrupts the network and/or telecommunications, reestablishing the connectivity and telephony will be a high priority and a prerequisite for any IT recovery. Recovery of these services will be accomplished in parallel or immediately following recovery of the datacenter. As such, Information Technology is required to have detailed information and records on the configuration of the networking equipment. Detailed information of switches and routers is documented in our monitoring system and infrastructure website. The infrastructure and telecomm staff are responsible for keeping the hardware inventory up to date.

6.4 Application Recovery Information:

Information necessary for the recovery and proper configuration of all application software located on the central servers is critical to assure that applications are recovered in the identical configuration as they existed prior to the disaster. Detailed information on critical central applications will be documented in our monitoring system and infrastructure website. The infrastructure staff is responsible for keeping the software inventory up to date.

6.5 Desktop Equipment Recovery Information:

Information necessary for the recovery and proper configuration of all desktop computers and printers supported by Information Technology Services is critical to assure that client systems can be restored to a configuration equivalent to pre-disaster status. Detailed information on client systems (both PC and MAC) is documented in our monitoring system, infrastructure website, and Microsoft System Center Configuration Management database. The infrastructure staff is responsible for keeping the hardware inventory up to date.

Section 7: Disaster Recovery Processes and Procedures

7.1 Emergency Response:

The requirement for Crisis Management Team (CMT) involvement and the membership of the CMT will be dependent on the size and type of the incident. In addition, the actions of the CMT will be accomplished prior to the execution of this plan. Operations of the CMT are detailed in the MVSU Emergency Operations Plan. Examples of situations that may result in the involvement of the CMT include:

Severe structural damage to the facility where personal safety is in question, and where analysis must be completed to assure the building is acceptable for access. This would include, but is not limited to, damage from a flood or tornado.

Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contamination where the situation must be contained prior to building occupancy. Flooding or other situations which may pose the risk of electrical shock or other life-threatening situations.

Examples of situations that may not result in the involvement of the CMT include:
Major system/hardware failures that do not pose a hazard to personnel or property.
Utility outages (electrical, etc.) which are remote to the datacenter being affected.
For any situation/incident which requires the involvement of the CMT; the IT Incident Commander, Incident Command Team, nor any Crisis Management Team member will access the facility until the CMT leader has authorized access.

7.2 Incident Command Team:

The role of the IT Incident Command Team (under the direction of the Incident Commander) is to coordinate activities from initial notification to recovery completion. Primary initial activities of the team are:

Incident Occurrence: upon the occurrence of an incident affecting the IT services at Mississippi Valley State University, campus security and/or other individuals will notify the President and Cabinet. Personnel reporting the incident will provide a high-level assessment as to the size and extent of the damage. Based on this information, the Chief Information Officer will assume his/her responsibilities as the Incident Commander, and will contact the other members of the ICT, and provide them with the following basic information:

- Brief overview of the incident, buildings affected, etc.
- Which Incident Command Headquarters (ICH) will be used
- Scheduled time to meet at the ICH for initial briefing
- Any additional information beneficial at this point. No other staff members are to be contacted at this point, unless directed by the Incident Commander.

Incident Command Headquarters (ICH) location is: Annex I Building

Should this facility be rendered unusable, it is assumed that the disaster was "catastrophic" in nature and that the technology recovery effort will be secondary to other concerns. At this point, the IT Incident Commander (IC) will work closely with overall MVSU Crisis Management Team. The IT IC is responsible for locating an alternate site for the team and re-evaluating the best strategy for recovery.

Incident Assessment: The Incident Command Team (ICT) will receive an initial briefing from the Incident Commander (IC) and any other personnel invited to the meeting (CMT personnel, etc.) The ICT will assess the situation, perform a walk-through of affected areas as allowed, and make a joint determination as to the extent of the damage and required recovery effort. Based on this assessment, the team will make a determination as to whether the situation can be classified as "routine" and handled expeditiously via normal processes, or if a formal IT disaster needs to be declared.

ROUTINE: Area(s) affected by the incident are identified and the appropriate personnel are contacted to report to work to evaluate and resolve the situation.

DISASTER: The Incident Commander contacts the MVSU Crisis Management Team and notifies them of the situation, and that an IT Disaster has been declared. The ICT identifies which areas of the IT infrastructure are affected, and contacts the members of the Disaster Recovery Team. Team members are provided with the following information:

- Brief overview of what occurred

  Location and time for teams to meet

Additional information as required. Team members are not to discuss any information provided with other personnel employed or not employed at Mississippi Valley State University.

Once an IT disaster has been declared, and the preceding steps to notify the MVSU Crisis Management Team have been accomplished, ongoing responsibilities of the Incident Command Team and Incident Commander include:

- Securing all IT facilities involved in the incident to prevent personnel injury and minimize additional hardware/software damage.
- Supervise, coordinate, communicate, and prioritize all recovery activities with all other internal / external agencies. Oversee the consolidated IT Disaster Recovery plan and monitor execution.
- Hold regular Disaster Recovery Team meetings/briefings with team leads and designees.
- Appointing and replacing members of the individual recovery teams who are absent, disabled, ill or otherwise unable to participate in the process.
- Provide regular updates to the MVSU Crisis Management Team on the status of the recovery effort. Only the MVSU Crisis Management Team and/or their designees will provide updates to other campus and external agencies (media, etc.)

- Approve and acquire recovery resources identified by individual recovery teams.
- Interface with other activities and authorities directly involved in the disaster recovery (Police, Fire, Department of Public Works, etc.)
- Identify and acquire additional resources necessary to support the overall disaster recovery effort, including acquiring backup generators and utilities, and arranging for food/refreshments for recovery teams, etc.
- Make final determination and assessment as to recovery status, and determine when IT services can resume at a sufficient level.

7.3 Disaster Recovery Teams:

The Disaster Recovery Teams are organized to respond to disasters of various type, size, and location. Any or all of these teams may be mobilized depending on the parameters of the disaster. It is the responsibility of the ICT to determine which Disaster Recover Teams to mobilize, following the declaration of a disaster and notification of the MVSU Crisis Management Team.

Each team will utilize their respective procedures, disaster recovery information, technical expertise, and recovery tools to expeditiously and accurately return their systems to operational status. While recovery by multiple teams may be able to occur in parallel, the datacenter and network/telecommunications infrastructure will be assigned the highest priority, as full operational recovery of most other systems cannot occur until these areas are operational.

7.3.2 Datacenter Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery of datacenter.
3. If the alternate datacenter site is required, execute all necessary steps to notify appropriate personnel and secure backup facility.
4. Identify other individuals required to assist in recovery of datacenter, and report this information to the IC for action
5. Develop overall recovery plan and schedule, focusing on highest priority servers for specific applications first.
6. Coordinate hardware and software replacements with vendors.
7. Recall backup/recovery tapes from on campus or off-campus storage, as required to return damaged systems to full performance.
8. Oversee recovery of datacenter based on established priorities.
9. Coordinate datacenter recovery with other recovery efforts on campus.

10. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
11. Verify and certify restoration of the datacenter to pre-disaster functionality.

7.3.3 Desktop, Lab, and Classroom Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage at all areas affected, and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of desktop services, and report this information to the IC for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure/desktop services first. (Appendix E documents the priority areas of the campus for IT service recovery)
5. Coordinate hardware and software replacement with vendors. (See Appendix F for vendor and contact information)
6. Oversee recovery of desktop computing services (workstations, printers, etc.) based on established priorities.
7. Coordinate recoveries with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the desktops to pre-disaster functionality.

7.3.4 Enterprise Systems Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery to Banner and enterprise systems.
3. Identify other individuals required to assist in recovery of these applications, and report this information to the IC for action.
4. Restore degraded system function at backup site and inform user community of the restrictions on usage and/or availability.
5. Coordinate software replacement with vendor as required.
6. Coordinate Banner services recovery with other recovery efforts.
7. Execute plan to restore Banner and enterprise system services to full function.

8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Banner and enterprise systems services to pre-disaster functionality.

7.3.5 Infrastructure and Web Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of services, and report this information to the IC for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first.
5. Coordinate hardware and software replacement with vendors
6. Oversee recovery of messaging, telecommunications and infrastructure services based on established priorities.
7. Coordinate messaging, network and web systems recovery with other recovery efforts on campus.
8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Messaging, Network and web infrastructure to pre-disaster functionality.

7.3.7 Telecommunications, Network, and Internet Services Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of these services, and report this information to the IC for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first.
5. Coordinate hardware/software replacement with vendor as required.
6. Oversee recovery of voice and infrastructure services based on established priorities.
7. Coordinate the voice and infrastructure services recovery with other recovery efforts.

8. Provide scheduled recovery status updates to the Incident Commander to ensure full understanding of the situation and the recovery effort.

9. Verify and certify restoration of the voice network to pre-disaster functionality.

7.4 General System/Application Recovery Procedures/Outline:

The following steps are guidelines for the restoration of systems located at Mississippi Valley State University. While the recovery team has specific duties and responsibilities as outlined in Section 7.3, coordination is required to restore operations to the users. While the coordination and extent of personnel involved will depend on the type and severity of the disaster, the following steps may be required:

It is implied in the procedure/outline below that steps are simply provided as a guideline. The magnitude and type of disaster, and the number of systems affected will require that certain steps be augmented (at the discretion of the Disaster Team Lead and Incident Command Team), and that other steps will not be applicable to the situation at hand.

1. Determine extent of damage and make determination as to the following:
    a. Primary Datacenter operational/recoverable?
        i. YES: Remain in primary datacenter and initiate recovery accordingly.
        ii. NO: Contact personnel responsible for alternate datacenter and take necessary steps to ready the facility.
    b. Network Operations Center operational/recoverable?
        i. YES: Utilize existing NOC for recovery.
        ii. NO: Contact personnel responsible for backup NOC and take necessary steps to redirect network routes and ready the backup facility.
    c. Determine extent of applications affected
        i. Banner and/or other Enterprise Applications
        ii. Authentication (Active Directory)
        iii. Web Services (www.mvsu.edu)
    d. Determine extent of desktop/client systems affected throughout the campus.
2. Secure facility as necessary to prevent personnel injury and further damage to IT systems.
    a. Shutdown any active components.
    b. Physically secure facilities (datacenter, communication closets, etc.) as necessary to prevent unauthorized access.
3. Retrieve most recent on-site or off-site back-up media for previous three back-ups. Prepare back-up media for transfer to primary or secondary datacenter, as determined during the initial assessment.
4. Verify operational ability of all equipment on-site in the affected area (servers, network

equipment, ancillary equipment, etc.). If equipment is not operational, initiate actions to repair or replace as needed.

5. Test systems, and communication equipment as required to validate physical operation and performance.
    a. Server testing
    b. Network testing
    c. Desktop/Client testing
6. Upon restoration of the datacenter and servers to operational state:
    a. Restore systems using virtualized images
    b. If necessary, load operating system and test/validate
    c. If necessary, load application software and test/validate
    d. If necessary, load data and verify integrity
7. Verify overall performance of specific system(s) and report readiness to Incident Command Team, Management Team, and user community

8.0 Network & Telecommunication Recovery Guidelines:

Servers and central application software are located in a central facility that can easily be assessed and secured for damage. Data networking and telecommunications, however, has equipment located in every facility at Mississippi Valley State University as well as in the datacenter. Remote equipment is located in communication closets, often in multiple sites in a single building. In addition, data and telecommunication cabling runs throughout the campus and buildings, making it susceptible to varying levels of damage.

Depending on the type and scope of the disaster, the Telecommunications, Network, and Internet Services Recovery Team will be involved in the following activities, to assess the overall damage and impact to the campus, and to assure a comprehensive plan for recovery:

1. Severe storms/wind
    a. Perform comprehensive cable, fiber, and communications line testing
    b. Assess all communication closets and racks/equipment for damage
2. Fire
    a. Evaluate all cable and fiber in the vicinity of the fire for potential destruction or deterioration
    b. Test primary copper data feeds for destruction or deterioration
    c. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water, smoke, or other agents.

d. Assess all equipment with air filtration systems to assure adequate ventilation remains.

3. Water/Flood

a. Evaluate all cable and fiber in the vicinity of the water/flood for potential destruction or deterioration.

b. Test primary copper data feeds for destruction or deterioration

c. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water or other agents.

d. Assess all equipment with air filtration systems to assure adequate ventilation remains.

4. Earthquake

a. Evaluate all cable and fiber for potential destruction or deterioration

b. Test primary copper data feeds for destruction or deterioration

c. Ensure all networking equipment and equipment racks are securely attached

d. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water, smoke, or other agents.

Appendix A: Mississippi Valley State University IT Recovery Priority List

The following priorities have been established by the Department of Information Technology with consultation with the campus community.

A.1 IT Infrastructure Priorities:

This establishes the internal priorities for recovering the major infrastructure components for IT services. These priorities are based on the relationship between these systems, and the prerequisite nature of many of the items in order to be able to return full services to the campus.

1. Datacenter (main or alternative)
2. Infrastructure Services (as prioritized below)
3. Banner
4. Authentication Services
5. Web Services
6. Online Course Delivery
7. Desktop, Lab, and Classroom Technology

A.2 IT System Priorities:

Outlined below are the priorities for recovering IT services for specific customers and facilities across the campus. While the datacenter, web, and authentication services are centrally located and will be recovered for all users simultaneously, recovery of network and desktop services will be accomplished based on the following priorities, in order to return critical campus systems and facilities to operational status at the earliest possible time.

The current list of servers and priorities are maintained in OneDrive (access restricted).

All systems are prioritized for recovery using these criteria:
(1) Critical – Basic infrastructure and must be restored as soon as possible.
(2) High – Systems of extreme importance, but do not provide infrastructure.
(3) Medium – Important systems and applications, but do not have university-wide impact.
(4) Low – Systems important to specific departments or specific small populations of users.
(5) Full –Systems that may not be restored to functional status until normal operations are reestablished.

Review

This plan will be reviewed annually by the IT Director and updated as needed.

A.3 Contact Information

Name	Job Title	Phone Number	Email Address
	IT Director		
Carmela Staten	Assistant Director	662-254-3649	carmela@mvsu.edu
Steven Pitchford	Network Manager	662-254-8401	steven@mvsu.edu
Carrissa Pruitt	Programmer	662-254-3910	cpruitt@mvsu.edu
Brian Phillips	Network Technician	662-254-8404	brian.phillips@mvsu.edu
Dewon Hall	Webmaster	662-254-3724	dewon.hall@mvsu.edu
	Computer Technician		
Deborah Boyd	Office Manager	662-254-3744	Debra.boyd@mvsu.edu

A.4 Mississippi Valley State University Crisis Management Team Contact List

	Company	Position	Contact Number
1	MVSU	Chief of Police	662-254-3107
2	MVSU	President	662-254-3425
3	MVSU	VP Academic Affairs	662-392-8455
4	IHL	Risk Management	601-624-5306
5	IHL	Loss Control Safety	601-941-8602
6	MS Bureau of Investigations	Investigator	662-392-5494
7	MHP	Special Operations Group	601-754-7415
8	MS Bureau of Investigations	Lt., Investigator	662-582-6151
9	MVSU	Director, Communication & Marketing	662-719-3627
10	MVSU	Captain, MVSU Police	662-254-3478
11	MVSU	Chief of Staff	662-392-5662
12	MVSU	VP, Enrollment Mang.	662-299-2789
13	MVSU	Director, Facilities Management	662-254-3584/662-392-3196
14	Leflore County Civic Center		662-453-4065
15	MVSU	Director, Student Health	
16	Leflore County	Director, EMA	662-897-9517 662-392-0204
17	MVSU/City of Itta Bena	Grounds/Fireman	662-457-7393
18	MHP – Troop D	Trooper – Public Affairs	662-897-0224
19	MVSU	Director, Information Technology	662-254-3744
20	Leflore Co. Sheriff Dept.	Deputy Sheriff	662-897-6901
21	MVSU	Director, Purchasing Dept.	662-392-5131
22	MVSU	Sr. Accountant/Bursars	662-254-3316
23	MVSU	Supervisor, A/P	662-207-7289
24	MVSU	Fire Safety	662-392-8318
25	MVSU	CFO/MVSU	662-897-8503
26	MVSU	Director, HR	662-392-2849
27	Thompson Hospitality	Director, Food Service	803-381-7150
28	MVSU	Director of Counseling	662-254-3831
29	MVSU	Director, Housing	662-392-0855
30	City of Itta Bena	Fire Chief	662-254-0031
31	City of Greenwood	Fire Chief	662-455-7610
32	MEMA	Director	886-519-6362
33	FEMA – Regional IV	Administrator	770-220-5200