INFORMATION TECHNOLOGY SERVICES
DISASTER RECOVERY PLAN

Westfield
STATE UNIVERSITY

Revision History

Revision	Change	Date
1.0	DRAFT Disaster Recovery Plan	8/8/2006
1.1	FINAL Disaster Recovery Plan	10/12/2009
2.0	Reviewed	10/15/2009
2.1	Reviewed	10/22/2012
3.0	Reviewed and updated by Security Policy Team and CIO	10/19/2015
3.1	Reviewed and updated by Security Policy Team and CIO	9/5/2018

Section 1: Introduction

Faculty, staff and students of Westfield State University all rely heavily on the technological infrastructure and services to accomplish their work and as an integral part of the learning environment.

As a result of this reliance, technology services are considered a critical component in the daily operations of Westfield 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 Westfield State University is managed by the university's Emergency Response Team. Their actions are governed by the Westfield State University Emergency Response Plan.

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

This plan is required to be reviewed and updated, at a minimum, every 3 years by the Security Policy Team and approved by the Chief Information Officer.

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 Information Technology Services and that are critical for business continuity. This includes the following major areas:

- Authentication, single-sign-on, and network directory services
- On-premises enterprise applications (e.g. Banner)
- Datacenter (Wilson and Horace Mann)
- On-premises website and services
- Desktop equipment, labs, classrooms
- Data networks and telecommunications (wired and wireless networks, file services, 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 Information Technology Services department, but this plan will address restoration of connectivity and integration with these services. This includes the following major services:

- Hosted enterprise applications, including payroll, Office 365
- Learning Management System (Blackboard)
- Student Email (Exchange – O365)

This plan covers all phases of any technology related disaster occurring at Westfield 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 this 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. Information Technology will encourage all other departments to have contingency plans and Business Continuity Plans for their operations, which include operating without information technology related 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 specific Disaster Recovery Teams under the guidance and approval of the Incident Commander and Incident Command Team.

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.
- Equipment Configuration: A database (either soft or hard copy) which documents the configuration information necessary to return any technology hardware to pre- disaster configurations. This includes hardware revisions, operating system revisions, and patch levels.
- 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 Command Headquarters: Location where the ICTs meet and coordinate all activities with regard to assessment and recovery. For the Information Technology Services Department, the headquarters are located at:
  - Primary: Wilson Hall Data Center
  - Secondary: Horace Mann Data Center
  - Backup 1: Loughman Living Room
  - Backup 2: Horace Mann Center – Garden Room A
- 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 technology related recovery activities. For Westfield State University, the Incident Commander is the Chief Information Officer or designee(s).
- Incident: Any non-routine event which has the potential of disrupting technology services to Westfield State University.
- Major Disaster: A major disaster will be characterized by an expected downtime of more than 48 hours but less than 7 days.
- 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.
- Routine Incident: A routine incident is a technological 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.
- Web Services: All services related to Westfield State University's Internet and intranet web activities and presence.

Section 5: Teams - All Contact Information is located in University Emergency Response Handbook or by contacting the Information Technology Services Department.

5.0.1 Incident Commander

Chief Information Officer, Information Technology Services

5.0.2 Incident Command Team

Chief Information Officer, Information Technology Services
Associate Dean, Academic Information Services
Director, Administrative Systems
Executive Director, Infrastructure Services
Associate Director, Academic Technology Services
Webmaster, Marketing
Administrative Assistant, Information Technology Services

5.1 Infrastructure and Web Recovery Team

The Infrastructure and Web Recovery Team is composed of personnel within the Information Technology Services 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, for both voice and data. This includes but is not limited to 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 our 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 primary function of this working group is the restoration of the existing datacenter or the activation of the secondary datacenter depending on the severity of the disaster. 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 which impacts 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 or a functioning secondary site is a prerequisite for the recovery of most applications and IT services to the campus.

Team Lead:	Director, Infrastructure Services
Team Members:	Assistant Director, Infrastructure Services
	Webmaster, Marketing
	Network Engineer, Infrastructure Services
	Server Administrator, Infrastructure Services
	Support Desk Technicians (2)

5.2 Desktop, Lab, and Classroom Recovery Team

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 desktop systems, classrooms, and labs to usable condition. The team is not responsible for restoration of any data the user may have on their desktop computer. Westfield State University recommends all users store data files on our network 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 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 be accomplished with other recovery efforts on campus by the Incident Commander.

Team Lead:	Executive Director, Media Services
Team Members:	Associate Director, AIS
	Assistant Director, AIS
	Support Technicians (3)
	Student Technicians (3)

5.3 Enterprise Systems Recovery Team

The Enterprise Systems Recovery Team is composed of personnel within the Information Technology Services department that support out enterprise systems. The primary function of this 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.

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

Team Lead:	Director, Administrative Systems
Team Members:	Assistant Director, Administrative Systems (2)
	Programmer/Analysts (4)
	System Administrator
	Computing Coordinators supporting affected areas (business services, payroll, enrollment services, etc.) and Key Business Unit Personnel as needed by type of incident (payroll clerk, accountant, registrar, etc.)

5.4 Critical Westfield State University Contacts

A copy of the Westfield State University Emergency Response Contacts List is located in University Emergency Response Handbook or by contacting the Information Technology Services Department.

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 tape locations and retention periods summarized in the table below:

Type:	Location:
Infrastructure: Daily Backup (disk)	Parenzo 012B
Infrastructure: Weekly Backup (disk)	Parenzo 012B
Infrastructure: Exchange SIF’s (tape)	Bates Vault
Administrative Systems: Daily Backup (tape)	Wilson Data Center
Administrative Systems: Weekly Backup (tape)	Wilson Data Center
Administrative Systems: Monthly Backup (tape)	Bates Vault
Hot Recovery Site: Banner, Exchange partial SIF’s	Horace Mann Center

Westfield 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 deployed and managed by Westfield State University are backed up unless other arrangements have been made. As such, only data resident on these systems will be able to be recovered. In the event that a disaster occurs on the campus which 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 Services department highly recommends and encourages the use of network drives (on servers) to store all important files. The recovery of data not backed up to a network drive and/or full system backups are not covered under this plan.

6.1 Recovery Priorities

In the event of a disaster, the technological recovery priorities shall be as follows and are listed in priority order from highest priority to lowest:

1. **Datacenters and Servers:** 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 technological recovery. As such, the Information Technology Services department is responsible for keeping the hardware inventory up to date.
2. **Network and Telecom:** 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 technological recovery. Recovery of these services will be accomplished in parallel or immediately following recovery of the datacenter. As such, Information Technology Department is required to have detailed information and records on the configuration of the networking equipment. The Information Technology Services department operations staff are responsible for keeping the hardware inventory up to date and employing the services of our telecom vendor in order to restore service.
3. **Applications:** 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 and the teams from Information Technology Service and Academic Information Services are responsible for keeping the software inventory up to date.

4. **Desktops:** Information necessary for the recovery and proper configuration of all desktop computers and printers supported by Academic Information 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) and keeping the hardware inventory up to date is the responsibility of the staff of Academic Information Services.

Section 7: Disaster Recovery Processes and Procedures

7.1 Emergency Response:

The requirement for Emergency Response Team (ERT) involvement will be dependent on the size and type of the incident. In addition, the actions of the ERT will be accomplished prior to the execution of this plan. Operations of the ERT are detailed Reviewed and updated by Security Policy Team and CIO Emergency Operations Plan.

Examples of situations which will normally result in the involvement of the ERT 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 which will normally not result in the involvement of the ERT 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 ERT, the IT Incident Commander, Incident Command Team, nor any Emergency Response Team member will access the facility until the ERT Incident Commander 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 detailed in the University Emergency Response Plan and will include.

Incident Occurrence: Upon the occurrence of an incident affecting the technology services at Westfield State University, the President and Cabinet will be notified by campus security and/or other individuals and provide a high-level assessment as to magnitude of the impact. Based on this information, the Chief Information Officer will assume their 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
- Which Incident Command Headquarters (ICH) will be used
- Scheduled time to meet at the ICH for initial briefing
- No other staff members are to be contacted

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 (ERT 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 SOU Emergency Response Team and notifies them of the situation, and that an IT Disaster has been declared. The ICT identifies which areas of infrastructure are affected, and contact the members of the recovery teams. 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 Westfield State University.

Once an IT disaster has been declared, and the preceding steps to notify the University Emergency Response 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.
- Monitor and manage the consolidated IT Disaster Recovery plan 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 SOU Emergency Response Team on the status of the recovery effort. Only the SOU Emergency Response 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
- Identify additional resources necessary to support the overall disaster recovery effort.
  - Acquiring backup generators and utilities;
  - Arranging for food/refreshments for recovery teams.
- Make final determination and assessment as to recovery status, and determine when technology 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 and or augment with other resources, following the declaration of a disaster and notification of the University Emergency Response 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 normally be assigned the highest priority, as full operational recovery of most other systems cannot occur until these areas are operational.

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. 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 priorities 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, voice, network, application and desktop, if applicable, based on established priorities.
9. Coordinate datacenter, voice, network, application and desktop 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. Restore degraded system function at backup site and inform user community of the restrictions on usage and/or availability.
12. Verify and certify restoration of the datacenter to pre-disaster functionality.

7.4 General System/Application Recovery Guideline:

The following steps are guidelines to be followed for the overall restoration of systems located at Westfield State University. While each recovery team has specific duties and responsibilities, coordination between the various teams 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:***

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
        iii. 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
            1. Authentication (Active Directory Services)
        ii. Web Services (westfield.ma.edu)
    d. Determine extent of desktop/client systems affected throughout the campus.
    e. Perform comprehensive cable, fiber, and communications line testing
    f. Evaluate all cable and fiber in the vicinity of the fire for potential destruction or deterioration
    g. Test primary copper data feeds for destruction or deterioration
    h. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water, smoke, or other agents.
    i. Assess all equipment with air filtration systems to assure adequate ventilation remains.
    j. Test primary copper data feeds for destruction or deterioration
    k. Ensure all networking equipment and equipment racks are securely attached

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 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.
    - i. Server testing
    - ii. Network testing
    - iii. Desktop/Client testing
    - iv. Upon restoration of the datacenter and servers to operational state:
    - v. Restore systems using virtualized images
        1. If necessary, load operating system and test/validate
        2. If necessary, load application software and test/validate
        3. If necessary, load data and verify integrity
    - vi. Verify overall performance of specific system(s) and report readiness to Incident Command Team, Management Team, and user community.
    - vii. Perform comprehensive cable, fiber, and communications line testing
    - viii. Evaluate all cable and fiber in the vicinity of the fire for potential destruction or deterioration
    - ix. Test primary copper data feeds for destruction or deterioration
    - x. Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water, smoke, or other agents.
    - xi. Assess all equipment with air filtration systems to assure adequate ventilation remains.
    - xii. Test primary copper data feeds for destruction or deterioration
    - xiii. Ensure all networking equipment and equipment racks are securely attached