DISASTER RESPONSE & RECOVERY PLANNING

Information Technology Services

Review Frequency: Annual **Review Schedule:** March 2016 **ADDITIONAL DETAILS** **Vendor list details redacted from this version.**	**Effective:** May 2006 **Last Update:** March 2015 **Responsible University Officer:** *Chief Information Officer*

Table of Contents

Introduction

Information Technology Services (ITS) recognizes that much of the University's day-to-day business depends on computers. The University's computers are linked together by a sophisticated network that provides connections with other machines across the campus and around the world. This network is also vital to telecommunications services at the University.

This dependency on computers and telecommunications for operational support poses the risk of a lengthy loss of capabilities should a disaster occur that damages the University's complex network of systems. Without adequate planning and preparation to deal with disasters, the University's core systems and services could be unavailable for many weeks.

Primary Focus

The primary focus of this document is to provide a strategy to respond to a disaster that severely cripples the University's core systems and services. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

At this time the University of West Georgia outsources faculty, staff, and student email and calendar service. In the event of a disaster that did not totally disrupt the campus network and/or the local cellular networks these services would remain available. Currently, the University does not run other mission critical services on redundant servers which would minimize potential business disruption in the event of a disaster. The university does have an off site location for the storage of backup data. This site has the potential to function as a temporary data center at the time of a disaster, or if funds were available, to be developed as a fully functional hot site.

Objectives

ITS' strategy has the following objectives:

1. Identify measures that prevent or lessen the impact of a disaster.
2. Provide information concerning personnel that will be required to restore core systems and services.
3. Identify core systems and services.
4. Organize core system, core service, and key personnel information to aid in an orderly course of action for restoring core systems and services.

Scope

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

Core Systems
The Data Center
DNS, DHCP, and Firewalls
Networking
Telecommunications (PBX)

Mission Critical Systems – Local*
** these services depend on the core systems plus local servers to be in a production state in order to be functional*
Active Directory
Banner Student Information System
Main Campus Web Services
Luminis Portal

Mission Critical Systems – Outsourced*
** these services depend on the core systems, or an alternate work location with adequate internet connectivity, to be functional*
Human Resources (ADP)
Payroll (ADP)
Financials (USG Peoplesoft)
Email and Calendaring (Google)
Learning management System (USG Desire2Learn)

Mission Supportive Systems
Desktop Equipment, Labs, Classrooms, File Servers
Department Level Systems and Services

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 DRRP.
- The safety of students, staff and faculty are of prime 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 Services encourages 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 specific IT Disaster Recovery Team under the guidance and approval of the Chief Information Officer (CIO) or designee.

Prevention and Detection

The best way to prepare for a disaster is to avoid the disaster. While Information Technology Services cannot guarantee against a disaster, efforts have been made to prevent and limit the impact of certain disasters. The following items have been addressed by ITS to prevent and mitigate the impact of a disaster to systems and services under ITS control.

Description	Location and Measures Taken
Central Data Center room – houses the University's mission critical servers and core network equipment.	• Electrical power for core systems and services is managed to look for and eliminate any obviously overloaded electrical circuits. • Physical security is provided as follows: two (2) entry doors located in the interior of the Boyd building. There are no external doors located in the Data Center. Both doors are protected by a card swipe and numeric key lock. The Data Center is also protected by an alarm system. University Police Second Shift ensures that the Boyd building's external doors are locked at night. They also ensure that the Data Center's internal doors are locked and the Center's alarm system is set. The Data Center also has a 24-hour alarm system with motion detectors. Two video surveillance cameras record activities in the room. Recordings are maintained for 1 month. • Fire Safety is provided by an automatic sensing Fenwal Protection System FM200 Clean Agent Fire Suppression System as well as follows: two (2) Carbon Dioxide handheld fire extinguishers located outside of the Data Center at each entry door; two (2) Carbon Dioxide handheld fire extinguishers located inside of the Data Center at each entry door; smoke detectors with 24-hour alarms. • Water Safety is provided as follows: a 24-hour alarm system with water detection sensors located on the floor of the Data Center. • Environmental Control is provided as follows: two (2) closed system air conditioning units provide cooling and humidity control for the Data Center. • Power Protection is provided as follows: electrical power is "conditioned" through 24-hour uninterruptible Power Supply (UPS) systems that provided uninterrupted electrical power for brief interruptions or allow time for the Data Center's electrical system to be transferred to generator supplied power or for proper shutdown of individual computers or network devices. • Redundant natural gas powered generators supply power in the event of a power outage.

Description	Location and Measures Taken
Central PBX – is integrated into Central Data Center room	• Please see information on Central Data Center room.
Secondary Data Rooms	• While not considered data centers, secondary data rooms are located around campus, and may be used as temporary data centers during a disaster. Current locations are: ○ Humanities 135. This area has a dedicated A/C unit, card swipe and keypad access control, and limited battery backup. An alarm system is in place and monitored by University Police. Temperature sensors are also installed. ○ Aycock Hall Second Floor room TC. This area has a dedicated A/C unit, card swipe access control, a fire alarm monitored by University Police, battery backup, and generator power. Temperature sensors are also installed.
Off Site Data Center	• An off site data center provides a location for redundant data backups and file storage. The facility provides: ○ redundant diesel generators ○ redundant cooling systems and 24hr temperature monitoring ○ FM-200 fire protection ○ card access with picture ID access control ○ video surveillance ○ ability to rent additional data center space ○ ability to rent office and work space ○ ability to provide alternative internet connectivity
Network Wiring Closets – houses network devices, switches, and wire management.	Location: These closets are located throughout the University. Physical Security: With few exceptions wiring closets are protected by keyed lock doors. A current listing of network wiring closets can be found on the department file server under its-dept\data\Networking\AAA Networking Continuity. A printed list is also retained with a copy of this DR Plan in Boyd 103.
Weather Monitoring	University Police monitors weather reports and coordinates communications to the campus concerning severe weather. A weather radio is installed in Cobb Hall that can be used to track storm warnings and progress.

Employee Contact Data Collection

A key factor in successful disaster recovery efforts is the ability to contact people. Information Technology Services uses the following methodology to record ITS employee contact information:

Data Collected

The following information should be collected for ITS employees:

- Name
- Address
- Home telephone number
- Pager number, if available
- Cellular telephone number, if available
- Primary email address (this should be a westga.edu address)
- Alternate email address (this should be a non westga.edu email address)
- Alternate contact information

Home street address is needed in case telephones are out of order and someone must be dispatched to physically locate the employee.

Alternate method of contacting the employee in the event of an emergency should include the name of a person to call, the relationship of that person (spouse, parent, son, daughter, neighbor, etc.), and a phone number where the person is most likely to be reached.

If employees do not have pagers or cellular phones - leave those entries blank.

Some staff members may be concerned about having their home information published. They may, for example, have an unlisted home number. It is essential that all employees provide a means to be contacted following an incident. These team members must be assured that this information will only be distributed on a “need to know” basis, and that the information will be secured.

This information is most easily gathered by distributing the Employee Data Collection Form (see Appendix B) to the employees for them to complete. The information gathered can be maintained with the non-public version of this plan.

A copy of the DRRP and the employee contact information is housed in the following locations. Contact information is verified or updated annually:

UWG file server: its-dept\Emergency Contacts
Boyd Building Room 104 safe
Cobb Hall Room 205 filing cabinet

Emergency Notification System

ITS expects to use the e-mail, telephone, and other contact information collected to reach employees in the event of a disaster. The University also maintains an emergency notification service that may also be used to call, text or email employees.

Information for Contacting Vendors

Product or service provided
Name of the vendor
Contact person's name
Contact phone numbers
Alternate names and numbers for the vendor
Comments

Product or service provided should be a description of the product or service provided to you. Along with "Comments", this helps to indicate the reason that this vendor should be contacted following the event.

For some vendors, there may not be a specific contact person's name to list. The "Service Representative on Call" may be appropriate response in some cases. In other cases, a title or department, such as "Sales Representative" or "Service Department" may suffice.

Contact phone numbers should include all possible ways to reach the vendor including fax, cellular, pager, after hours number if different from the normal number and toll-free numbers in addition to the normal number.

Alternate names and numbers should also be listed wherever possible. Alternate names are alternates to the primary contact person's name, if listed.

Some vendors may not have 24-hour service. If your incident occurred on a Sunday afternoon, you might need to contact the vendor at that time. Discuss your concerns with the vendor representative to determine how to contact them during off-hours. After reassuring him or her that the information will have limited distribution, ask for home telephone numbers if cellular or pager numbers are not sufficient.

Comments can be used for any information significant to this vendor, such as the reason this vendor should be contacted following an incident, instructions the vendor would need or any appropriate notes.

See Appendix A for current vendor list.

Meeting Location

During a disaster key ITS personnel need to know where to meet. The following is a pre-defined list of locations:

- Primary Location – Room 104 Boyd Building, University of West Georgia Campus. This room is located directly across from the University's main Data Center.

- Secondary Location – Room 207 Cobb Hall, University of West Georgia Campus. This location houses ITS personnel.

Restoration Resources

The intent of disaster recovery efforts by ITS is to restore operations as quickly as possible. In order to do this ITS' strategy includes the following goals:

- Identify core systems and services.
- Organize core system, core service, and key personnel information to aid in an orderly course of action for restoring core systems and services.

  ITS maintains individual information security plans that document IT systems and services, key personnel responsible for the service, hardware dependencies, and strategies for restoration. The plans are stored on the UWG file server under its-dept\IT Systems.

Emergency Response

The response to and recovery from a campus wide emergency that cannot be managed through normal channels is governed by the campus Emergency Management Plan. The requirement for a campus incident command group and the membership of that group will be dependent on the size and type of the incident. In addition, the actions of the campus incident command group will be accomplished prior to the execution of this IT recovery plan. Examples of situations that will normally result in the involvement of the campus command group 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 hurricane or tornado.
- Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contaminations where the situation must be contained prior to building occupancy.
- Flooding or other situations that may pose the risk of electrical shock or other life-threatening situations.

Examples of situations that do not normally result in the involvement of the campus incident command group include:

- Major system/hardware failures that do not pose a hazard to personnel or property.
- Utility outages (electrical, etc.) that are remote to the Data Center.

NOTE: For any situation/incident that requires the involvement of a campus incident command group, neither the IT Incident Director, Incident Command Team nor any Disaster Recovery Team member will access the facility until the campus incident

command group leader has authorized access. For more information on the campus incident command group, see the Emergency Management Plan, http://www.westga.edu/assetsDept/pubsafe/all_hazard2013.pdf.

IT Disaster Recovery Team (IT DR Team)

Contact information for team members can be found on the alert list.

Chain of Command
Chief Information Officer, then
Director of Enterprise Technical Services, then
Director of User Services, then
Director of Enterprise Applications

Primary IT DR Team Members and Roles
Director of User Services for external communications
Lead Project Manager for project management
Director of Enterprise Technical Services for infrastructure
Director of Enterprise Application Services for enterprise applications
Manager of Systems Administration
Manager of Network Services
Manager of Web Innovations

IT DR Team

The role of the IT DR Team 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 UWG, the President, and Chief Information Officer will be notified by campus security and/or other individuals. Personnel reporting the incident will provide a high-level assessment as to the size and extent of the damage. Based on this information, the CIO will contact the other members of the DR Team, and provide them with the following basic information:

- Brief overview of the incident, buildings affected, etc.
- Which meeting location will be used
- Scheduled time to meet for initial briefing
- Any additional information beneficial at this point.

Meeting locations are:

- Primary: ITS Boyd Operations Center (Boyd 104)
- Secondary: Cobb Hall Conference Room (Cobb 207)

Should both of these facilities 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 CIO or designee will work closely with overall UWG management to determine the appropriate course of action. The CIO or designee is responsible for locating an alternate site for the team and re-evaluating the best strategy for recovery.

Incident Assessment and Actions

IT DR Teams are organized to respond to disasters of various type, size, and location. Any or all personnel may be mobilized depending on the parameters of the disaster.

The IT DR Team will receive an initial briefing from appropriate personnel and assess the situation, including performing 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. Service restoration can occur within 48 hours either via temporary or permanent means.
>
> **DISASTER**: Service restoration time via either temporary or permanent means exceeds 48 hours. The CIO or designee contacts UWG management (President or designee) and notifies him/her of the situation, and that an IT Disaster has been declared. The IT DR team identifies which areas of the IT infrastructure are affected, and contacts any additional personnel required to address the situation. 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 UWG.

Once an IT disaster has been declared, and the preceding steps to notify UWG management and additional IT DR team members have been accomplished, ongoing responsibilities of the IT DR Team 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 IT DR 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 UWG management on the status of the recovery effort. Only UWG management 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, other UWG Teams, etc.)
- Identify and acquire additional resources necessary to support the overall disaster recovery effort. These can include 1) acquiring backup generators and utilities, 2) 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.

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 Data Center and Core 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.

Data Center Recovery

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 central Data Center Facility. Determine if use of secondary or off-site data center is required.
3. If the off-site data center site is required, execute all necessary steps to notify appropriate personnel and secure additional space or resources at the off-site facility.
4. Identify other individuals required to assist in recovery of data center, and report this information to the ID for action.
5. Develop overall recovery plan and schedule, focusing on highest priority servers for specific applications first. (Core Services, then Mission Critical, followed by Mission Supportive Services)
6. Coordinate hardware and software replacements with vendors. (See Appendix A for vendor and contact information)
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 data center based on established priorities in step 5.
9. Coordinate data center recovery with other recovery efforts on campus.
10. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
11. Verify and certify restoration of the data center to pre-disaster functionality.

Telecommunications and Networking

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 ID for action.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the campus infrastructure first. (Core Services, then Mission Critical, followed by Mission Supportive Services.)
5. Coordinate hardware/software replacement with vendor as required. (See Appendix A for vendor and contact information)
6. Oversee recovery of voice network services based on established priorities.
7. Coordinate the voice network recovery with other recovery efforts.
8. Provide scheduled recovery status updates to the Incident Director to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the voice network to pre-disaster functionality.

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

1) Natural Disaster/Water/Flood
   a) Perform comprehensive cable, fiber, and communications line testing.
   b) Assess all communication closets and racks/equipment for damage.
   c) Evaluate all cable and fiber in the vicinity of the water/flood for potential destruction or deterioration.
   d) Test primary copper data feeds for destruction of deterioration.
   e) Evaluate and test/assess all electronic equipment (hubs, switches, routers, etc.) that have been exposed to water or other agents.
   f) Assess all equipment with air filtration systems to assure adequate ventilation remains.

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 of 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.

General System Recovery

The following steps are guidelines to be followed for the overall restoration of systems located at UWG. The individual information security plan documents can be used to

assist in the recovery effort.

While the coordination and extent of personnel involved will depend on the type and severity of the disaster, the following steps may be required:

NOTE: 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, 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 Data Center and core network operational/recoverable within 48 hours?
        i. YES: Remain in primary data center and initiate recovery actions accordingly.
        ii. NO: Investigate use of secondary data centers and off site data center.
    b) Determine extent of applications affected
        i. Banner Student Information System
        ii. Main Web Services (www.westga.edu)
        iii. Other systems and file servers
    c) Determine extent of desktop/client/network 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 (Data Center, wiring closets, etc.) as necessary to prevent unauthorized access.

3. Retrieve most recent on-site or off-site back-up media. Prepare back-up media for transfer to primary or secondary data center 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) Network testing
    b) Server testing
    c) Desktop/Client testing

6. Upon restoration of the Data Center and servers to operational state:
    a) Load Operating System and test/validate
    b) Load Application Software and test/validate

c) Load Data and verify integrity

7. Verify overall performance of specific system(s) and report readiness to the IT DR Team, campus incident command group, and user community.

Appendix A Vendor List

Vendor List Redacted

Appendix B Employee Contact Data Collection Form

UWG ITS Employee Contact Data Collection Form

Date the following information was provided: _____

Name: _____

Title: _____

Address: _____

City/State/Zip: _____

Office Phone: _____ Home Phone: _____

Pager: _____ Cellular: _____

Campus Email address: _____

Non Westga.edu E-mail: _____

Alternate method(s) to contact employee in an emergency (should include the name of a person to call, the relationship of that person (spouse, parent, son, daughter, neighbor, etc.), and a phone number where the person is most likely to be reached):
_____

_____

_____

_____

_____

_____

Please return the completed form to: _____

The information you provide will be a part of the ITS Disaster Response and Recovery Plan. In the event of a disaster, management may need to contact you to inform you of changes in work hours or locations. Your contact information will only be available within the non-public version of recovery plan and will have limited distribution.

Appendix C. Document Revision History

This document should be reviewed annually and updated as needed.

Date	Revision Summary	Revision Notes	Revision #
May 2006	Creation	Creation	0
September 2008	Updated and Reviewed	Review	1
May 2009	Reviewed	Review	2
September 2010	Reviewed	Review	3
April 2013	Reviewed	Review	4
October 2013	Updated and Review	Review	5
March 2014	Updated and Review	Review	6
March 2015	Minor Updates & Reviewed	Review	7

Appendix D Quick Action Check List

This checklist serves as a guide to the high-level actions needed to respond to an IT outage or disaster situation.

1. Evaluate the situation
    a. Notify emergency personnel if needed (University Police 678-839-6000)
    b. Take any steps necessary to ensure personnel safety
2. Notify ITS Management (CIO, ETS, EAS, and US Directors)
    a. Nature of disaster
    b. Location of disaster
    c. If possible, give a high level overview of next steps
3. Coordinate Initial Response
    a. Determine location for team to meet
    b. Contact primary team members
    c. Assess the situation
    d. Collect any equipment needed (computers, radios, batteries, phones, printers, software, etc.)
    e. Determine response
    f. Begin response
    g. Communicate status