DISASTER RESPONSE & RECOVERY PLANNING

Information Technology Services
## Table of Contents

Introduction .................................................................................................................. 1  
Primary Focus ............................................................................................................... 1  
Objectives ...................................................................................................................... 1  
Scope .............................................................................................................................. 2  
Assumptions .................................................................................................................... 2  
Prevention ....................................................................................................................... 3  
Employee Contact Data Collection .................................................................................. 4  
  Data Collected ........................................................................................................... 4  
  Emergency Notification System ................................................................................. 5  
Information for Contacting Vendors ............................................................................. 5  
Meeting Location .......................................................................................................... 6  
Restoration Documentation ........................................................................................... 6  
Emergency Response ...................................................................................................... 6  
IT Incident Director and Command Team ........................................................................ 7  
IT Incident Command Team (ICT) .................................................................................. 7  
Incident Assessment ....................................................................................................... 8  
Disaster Recovery .......................................................................................................... 9  
Data Center Recovery ..................................................................................................... 10  
Telecommunications and Networking .......................................................................... 10  
General System Recovery .............................................................................................. 11  
Appendix A Vendor List .................................................................................................. 13  
Appendix B Employee Contact Data Collection Form ................................................... 14  
Appendix C. Document Revision History and Update Plan ............................................. 15
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.

The response to and recovery from a disaster at the University of West Georgia is managed by the President, the Chief of University Police, and the Director of Facilities. This group is referred to as the campus Emergency Response Team (campus ERT) in this document. Their actions are governed by the UWG Emergency Operation Plans located at http://www.westga.edu/police/index_5162.php

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 does not run any mission critical services on redundant servers which would minimize potential business disruption in the event of a disaster, nor does the university possess a redundant “warm-site” or “hot-site” for quick recovery of the Data Center. Should more resources become available this plan will be re-evaluated and updated accordingly.

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.
ITS Disaster Response & Recovery Planning

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, and Telecommunications (PBX)

Mission Critical Systems
- Banner Student Information System
- Electronic Mail
- Main Campus Web Services
- Luminis Portal

Mission Supportive Systems
- Desktop Equipment, Labs, Classrooms, File Servers
- Facility Services (FME)
- Auxiliary Services (Parking, Health Services, ResNet)
- Support Services (remedy Helpdesk, RedDot Content Management)

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 Disaster Recovery Teams under the guidance and approval of the Incident Director and Incident Command Team.
Prevention

The best way to prepare for a disaster is to avoid the disaster. Information Technology Services cannot guarantee against a disaster. However, 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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Location and Measures Taken</th>
</tr>
</thead>
</table>
| 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 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. |
| Central PBX – is integrated into Central Data Center room | • Please see information on Central Data Center room. |
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.

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 quarterly:

Boyd Building Room 102 safe  
Cobb Hall Room 205 filing cabinet  
University Police Dispatch Office, Coliseum

**Emergency Notification System**

ITS expects to use the Schoolcast emergency notification system to alert employees of potential emergency or disaster situations. The Schoolcast system can send alerts via phone, email, or SMS message. Each ITS employee has an alternate email address (non westga.edu domain) and telephone number entered into the Schoolcast system.

The contact information in the Schoolcast system will be updated quarterly along with the alert list.

The Schoolcast system will be tested quarterly.

**Information for Contacting Vendors**

<table>
<thead>
<tr>
<th>Product or service provided</th>
<th>Name of the vendor</th>
<th>Contact person’s name</th>
<th>Contact phone numbers</th>
<th>Alternate names and numbers for the vendor</th>
<th>Comments</th>
</tr>
</thead>
</table>

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 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 106 Boyd Building, University of West Georgia Campus. This room is located directly across from the University’s Central Data Center and houses ITS’ Technical and Networking personnel.

• Secondary Location – Room 206 Cobb Hall, University of West Georgia Campus. This location houses ITS personnel.

Restoration Documentation
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.

The addendums at the end of this document are directly related to the fulfillment of these objectives. Realistic preventative measures have been identified and a table format was used to organize the information. Needed information concerning ITS personnel was identified and an explanatory narrative precedes a listing of the actual personnel contact list. Last and most importantly, this document contains listing of critical services and systems arranged in a "Data Sheet" format that identifies the service, key personnel responsible for the service, hardware and dependant services, and strategies for restoration.

Emergency Response
The requirement for a campus Emergency Response Team (campus ERT) involvement and the membership of the campus ERT will be dependent on the size and type of the incident. In addition, the actions of the campus ERT will be accomplished prior to the execution of this plan. Examples of situations that will normally result in the involvement of the campus ERT include:
ITS Disaster Response & Recovery Planning

- 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 which 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 ERT 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 ERT, neither the IT Incident Director, Incident Command Team nor any Disaster Recovery Team member will access the facility until the campus ERT leader has authorized access.

**IT Incident Director and Command Team**
Contact information for the incident director and command team can be found on the alert list.

**IT Incident Director**
Kathy Kral
Hugh Russell (first alternate)
Blake Adams (second alternate)

**IT Incident Command Team (ICT)**
Blake Adams (External Communications)
Dale Driver (Project Management)
Price Hall (Systems Administration)
Hugh Russell (Infrastructure)
Karen West (Enterprise Applications)
Rob Yawn (Networking)

**IT Incident Command Team (ICT)**
The role of the IT Incident Command Team (under the direction of the Incident Director) 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
ITS Disaster Response & Recovery Planning

assessment as to the size and extent of the damage. Based on this information, the CIO will assume his/her responsibilities as the Incident Director, 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 Director.

Incident Command Headquarters (ICH) locations are:

- Primary ICH: ITS Boyd Operations Center (Boyd 102)
- Secondary ICH: 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 IT Incident Director will work closely with overall UWG management to determine the appropriate course of action. The ID 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 Director (ID) and any other personnel invited to the meeting (campus 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, if a formal IT disaster needs to be declared, or if the situation is involves a total loss of the Boyd Data Center and is catastrophic in nature.

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.

CATASTROPY: if it is decided that the core services of Boyd Data Center cannot be recovered within 48 hours, the situation may be deemed a catastrophe by the campus ERT and ICT. In this situation outside resources including leased equipment, mobile data centers, and staffing etc. will be needed.

DISASTER: The Incident Director contacts UWG management (President or designee) and notifies him/her 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 required personnel to form the Disaster Recovery Team. Team members are provided with the following information:

- Brief overview of what occurred
ITS Disaster Response & Recovery Planning

- 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 the Disaster Recovery Teams have been accomplished, ongoing responsibilities of the Incident Command Team and Director 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 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.

**Disaster Recovery**

Disaster Recovery 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. It is the responsibility of the ICT to determine which personnel to mobilize, following the declaration of a disaster and notification by the campus ERT.

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 can not 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 Facility. Determine if use of alternate/cold site is required.
3. If the alternate data center 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 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 F 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.
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 F 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. 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 (at the discretion of the Disaster Recovery 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 Data Center and core network operational/recoverable within 48 hours?  
   i. YES: Remain in primary data center and initiate DRRP accordingly.  
   ii. NO: This situation may be classified as a catastrophe and not covered by this document. (the 2009 update should address this)  
b) Determine extent of applications affected  
   i. Banner Student Information System  
   ii. Messaging (Email)  
   iii. Web Services ([www.westga.edu](http://www.westga.edu))  
   iv. 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 for previous three back-ups. 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 Incident Command Team, Management Team, and user community.
Appendix A Vendor List

Vendor List

DELL
http://dell.com

EXTREME NETWORKS
John R. Greiner
Regional Sales Manager- GA, AL
Off: 770.353.5845
Cell: 404.556.6145
Fax: 678.482.4658
email: jgreiner@extremenetworks.com

University of Georgia SRS
http://www.srs.usg.edu

FloorCare Specialists, Inc.
www.floorcarespecialists.com

CanIT
www.roaringpenguin.com

STAPLES ACCOUNT# 0530321280
Customer # 2645353778
Carrollton Location 770-830-1554

SUN Sun Hardware, Software, Operating system, Veritas
http://support.oracle.com

Sun VAR

Charlie Pierce
Systems Alliance
Education Program Director
706-248-9556 Cell
cpierce@systemsalliance.com

*For Telecommunications Vendor Information see Telecommunications Addendum
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 and Update Plan

This document should be reviewed annually and updated as needed.

Original document created May, 2006
First revision September, 2008
Reviewed: May 2009 (response to catastrophic loss of data center).
Reviewed: September 2010
Next revision: September 2011

Resources: http://www.rentsysrecovery.com