Jacksonville University Information Technology Department
Disaster Recovery Plan

(Rev: July 2013)
Table of Contents

Introduction 3
Objectives/Constraints 4
Assumptions 4
Critical Systems 5
Incidents Requiring Action 5
Contingencies 6
Physical Safeguards 6
Types of Computer Service Disruptions 7
Normal Computer System Problems 7
Major Computer Problems 7
Air Conditioning 7
Recovery Team 8
Organization of the Disaster/Recovery Team 8
Disaster/Recovery Team Headquarters 8
Disaster Recovery Coordinator 8
Administrative Systems/Ops Recovery Team Leader Responsibilities 9
Preparing for a Disaster 9
General Procedures 9
General Disaster Recovery Plan Timeline 11
Hurricane Specific Timeline 11
Software Safeguards 12
Recovery Procedures 13
Central Facilities Recovery Plan 13
Administrative Services Recovery Plan 13
Degraded Operation from Central Site 14
Academic Services Recovery Plan 15
Degraded Service at Central Site 15
Administrative Microcomputer (PC) Recovery Plan 16
Computerized Classroom/Library & Cybercafe PC Recovery Plan 16
Emergency Procedures 17
Appendices
APPENDIX A - Emergency Call Lists 18
APPENDIX B – Contacts Defined by priority 19
APPENDIX C - Vendor Contact List 20
APPENDIX D - Alternate Client Services Facility 22
APPENDIX E - Off-site Storage 23
APPENDIX F – Server Room Startup Procedure 24
APPENDIX G – Financial System Startup Procedure 28
Introduction

Over the years Jacksonville University has set up a highly computerized operational environment. This includes the use of personal computers in offices, as well as many network servers and computer devices that provide much of the operational support for the administrative and academic units. The campus-wide network ties these various systems together and provides communications to the entire University.

The reliability of computers and computer-based systems has increased dramatically in the past few years, and those computer failures that do occur can normally be diagnosed automatically and repaired promptly using both local and remote diagnostic facilities. Many computer systems contain redundant parts, which improve their reliability and provide continual operation when some failures occur.

A trend is evolving to provide alternate sites near the central systems where any additional equipment needed can already be housed and critical on-line operations for the organization can be resumed in a reasonable time. Redundancy in the communications network and a tie-in to the alternate site or the ability to rapidly tie-in is an important part of the disaster plan. This type of site is called a “warm site”, as opposed to a “hot site”, which contains all equipment necessary to start immediate operations and is fully duplicating the primary site.

For the most part, the major problems that can cause a computing system to be inoperable for a length of time result from environmental problems related to computing systems. The various situations or incidents that can disable, partially or completely, or impair support of JU computing facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require repair and restoration funding from the university in order to repair or replace the affected systems. This plan assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery.
Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the Founders Server Room or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting different departments in the Information Technology Department (IT). However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the university, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the computing support given to JU users from IT, including academic and administrative systems under the stewardship of IT. The elements that concern PC’s are addressed; however, client-related functions not directly tied to computer support by IT are not addressed. Also, offices at JU should develop their own plan to deal with manual operations within their office, should computer and/or network services be disrupted. Due to cost factors and benefit considerations at this time, the alternatives of hot sites and contracts with disaster recovery companies is not considered feasible or necessary for JU.

All major computing systems that are vital for the daily operation of the University and under the stewardship of IT are maintained under service contracts with the equipment vendors. This ensures that routine maintenance problems will be addressed in a timely way with adequate resources. These contracts range from telephone support only to full hardware replacement.

Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. Senior technology staff members on site will make any special decisions for situations not covered in this plan needed at the time of an incident.

1. This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first on site following an incident will contact the Chief Information Officer, Information Technology and the Directors of each individual department for a determination of the need to declare an incident.

2. The senior technology staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that all faculty, staff, and students are evacuated if a dangerous situation is identified. If injuries have resulted or may occur as a result of the incident, immediate attention will be given to those persons injured. JU Campus Security and Physical Plant will be notified if necessary. If the situation allows, attention will be focused on shutting down systems, turning off power by pressing the emergency shut off, etc., but evacuation is the highest priority.
3. Once an incident, which is covered by this plan, has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper university authorities are notified.

4. Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable computer support to the university has been reestablished.

5. We are planning on a warm-site strategy to our alternate site (CSX), a warm site being an alternate location with sufficient hardware, duplicated from the primary site, on which backups can be restored to have the campus system running in a minimal amount of time, but in a degraded state. This is primarily due to the prohibitive cost factor of a hot site duplicating the total hardware and networking infrastructure of the campus network.

6. The total body of the IT staff will be notified immediately by telephone on the invoking of a disaster incident and will be required to work till the disaster incident is closed and staff told to stand down.

**Critical Systems**

Critical Systems include but are not limited to the following and are rated in order of priority to recovery:

1. Network communications / connectivity
2. DNS/Active Directory
3. Administrative System (ERP)
4. Email/Telephone
5. File/Print
6. Web Services
7. Academic Labs
8. Individual PCs

**Incidents Requiring Action**

This disaster recovery plan for JU will be invoked under one of the following circumstances:

1. An incident that has or may partially or completely disable the operations of JU’s central computing for a period of 24 hours.

2. An incident, which has impaired the use of computers and networks, managed by IT, due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all administrative systems that IT manages.

3. An incident, which was caused by problems with computers and/or networks, managed by IT and has resulted in the injury of one or more persons at JU.
Contingencies

General situations that can destroy or interrupt computer usually occur under the following major categories:

- Power/Air Conditioning Interruption
- Fire
- Water
- Weather and Natural Phenomenon
- Chemical or biological disaster
- Sabotage and Interdiction

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- Partial recovery - Operating at an alternate site off campus and/or other areas on campus with a degraded level of service for a period of time.
- Full recovery - Operating at the Founders Server Room, possibly with a degraded level of service for a period of time

Physical Safeguards

There are five entrances to the Founders Building. The entrances use standard door locks on all five entrances and these doors are kept open during working hours and locked at night.

There is one entrance into the IT Server Room Founders 13. This door is protected by a smart card lock.

Founders Building – Server Room Founders 13 houses most of our data servers. It is the hub for campus-wide data networks. There is no protection against water damage. The room is connected to the campus fire/smoke detection system. There is no protection or detection for water damage.

The equipment room is connected to a UPS system, located in the server room Founders 13. The UPS provides approximately 15 minutes of power during a power interruption and there is an automatic transfer switch that will start up the diesel generator to all the computer equipment in the Server Room. The Generator is capable of powering all of the equipment, including lights and A/C in Founders 13.

AITC Building – This building houses the backup hardware, data and virtual servers needed to permit limited operations from this location. The AITC building is a high security facility that has every type of protection data equipment needs such as: Fire, Water and Power Protection. Employee access to the JU IT services housed in the facility is via VPN to a Terminal Server over a 10 Mbit connection to the Internet. Web based services for all will also be available through this connection.
Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve JU's computing facilities. Additional information that may be needed is provided in the appendices of this document. Supporting documents contain additional hardware, software and vendor information.

Normal computer system problems

For most of the major hardware vendors represented on campus, as well as some of the software vendors, remote diagnostic testing is available for routine problems. For most routine hardware problems, Dell provides next day service for hardware replacement. The JU/Dell Education agreement for hardware provides support on a 24 x 7 basis.

Some minor hardware problems do not disrupt service. Maintenance is scheduled when convenient to repair/resolve these problems. The JU Server Room maintenance window is Sunday after 12:00 am till Monday 7:00 am. Most hardware problems disrupting the total operation of the computers should be fixed within 4 to 8 hours.

Major computer problems

It is not feasible to keep a supply of PC’s or high-cost items to meet every emergency. In cases where workstations are lost, these will be repurchased/leased using Repair and Replacement funds.

Air Conditioning

As this is a sealed room, it has no windows, and has only one small wall A/C as an alternate method of cooling. Only by opening all of the doors to the room and setting up small fans can the room temperature be maintained and then only on a cooler or cold day. On a warmer day, the computer room could reach a very warm state if the A/C were to fail. The primary air conditioning system to the Server Room has been tested to ensure all are functioning properly. The UPS and Generator also provide power to the Air Conditioning unit. IT staff will need to setup fans and open door should an A/C outage occur to prevent the Server Room from overheating. JU's Air Conditioning/Heating group from the Physical Plant is responsible for service of these units. They are periodically checked and serviced, for emergency problems physical plant is available nights and weekends. Response is usually within the three hour reported. Humidity factors are also a consideration in the Server Room environment but are controlled by the air conditioning system.
Recovery Team

In case of a disaster, the emergency call list will need to be used. General duties of the disaster recovery coordinator are discussed. Recovery team leaders have been assigned in each major area and general duties given. The team leader will make assignment of personnel in the major areas to specific tasks during the recovery stage over that area.

Organization of the Disaster/Recovery Team

Disaster Recovery Coordinators – Chief Information Officer, Information Technology, Physical Plant Director, Student Life Director and Registrar’s Director.


Disaster/Recovery Team Headquarters

1. If the Founders Building is usable, the recovery team will meet in the conference room Founders 3.

2. If the Founders Building room 3 is not usable and other rooms are, the team will meet in Founders 5 the systems and planning office.

3. If the Founders Building is hazardous or not usable, the team will meet on the third floor conference room of the Howard Building.

4. If the Howard 3rd floor conference room is not usable, the Disaster Recovery Coordinator will be responsible for locating another meeting place on campus.

5. If none of the campus facilities are usable, it is presumed that the disaster is of such proportions that recovery of computer support will take a lesser priority. The Disaster Recovery Coordinator will make appropriate arrangements.

Disaster Recovery Coordinator

The Chief Information Officer, Information Technology will serve as the Disaster Recovery Coordinator. The major responsibilities include:

1. Invoking the Disaster Recovery Plan.

2. Supervising the recovery activities.

3. Naming replacements, when needed, to fill in for any disabled or absent disaster recovery members. Any members who are out of town and are needed will be notified to return.

4. The VP, IT will keep users informed of the recovery activities.
Administrative Systems/Operations Recovery Team Leader Responsibilities

The Director of IT Operations will serve as Administrative Systems/Operations Recovery Team Leader. Responsibilities include:

1. Coordinating hardware and software replacement with the administrative hardware and software vendors.
2. Supervising moving backup media and materials from the off-site safe and using these for recovery when needed.
3. Coordinating recovery with affected departments.
4. Coordinating scheduling for administrative programming, production services, and computer scheduling.
5. Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

General Procedures

Responsibilities will be given by the VP, IT. That way ensuring each of following actions have been taken and that any updating needed is continued.

1. Maintaining and updating the disaster recovery plan.
2. Ensuring that all IT personnel are aware of their responsibilities in case of a disaster.
3. Ensuring that periodic scheduled rotation of backup media is being followed for the off-site storage facilities.
4. Maintaining and periodically updating disaster recovery materials, specifically documentation and systems information, stored in the off-site areas.
5. Maintaining a current status of equipment in the main equipment rooms in the Founders Server Room.
6. Informing all technology personnel of the appropriate emergency and evacuation procedures from the Founders Server Room.

7. Ensuring that all security warning systems and emergency lighting systems are functioning properly and are being periodically checked by operations personnel.

8. Ensuring that fire protection systems are functioning properly and that they are being checked periodically.

9. Ensuring that UPS and Generator systems are functioning properly and that they are being checked periodically.

10. Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.

11. Ensuring that the operations procedure manual is kept current.

12. Ensuring that proper temperatures are maintained in equipment areas.

**General Disaster Recovery Plan Timeline**

Based upon notification that an incident has occurred at any of the computer facilities on campus, the Disaster Recovery Coordinator or Senior Management staff member should notify all other senior management IT staff. Communications among these members is critical to the successful restoration and recovery from a disaster.

If emergency procedures have not been invoked, at the four-hour mark after initial notification of an incident in any of the computer facilities, the Disaster Recovery Plan will take effect and should follow the following timeline.

**Phase 1** – Within 4 hours of initial notification Insure that all staff have been evacuated from the site and are accounted for. Insure that the primary site has been secured. Insure that safety, fire authorities, physical plant have all been notified. Decide whether to reopen the primary site or move to an alternate site. Notify all IT staff of a disaster. IT staff should already know their primary recovery responsibilities and report-to locations. Notify other sites of the disaster.

**Phase 2** – Within 12 hours of initial notification Confirm funding is available for recovery plan requirements. Notify vendors of the disaster and order preliminary hardware replacement. Initiate transportation of supplies and hardware to a recovery site. Initiate transportation of recovery media and hardware systems to a new site.

**Phase 3** – Within 24 hours of initial notification Restore system backups and test system integrity.
Insure sufficient supplies and needs at recovery site.
Bring up all recovery systems.
Establish backup schedules of all recovery systems.
Notify all IT staff and administration of operations at recovery site.
Inventory salvageable materials at primary site.
Reassess damages and loss at primary site.

Phase 4 – Within 48 hours of initial notification
Debrief staff on causes and results.
Decision – move back or stay at recovery site.
Prepare for disaster at recovery site.

Phase 5 – Within a specified time limit designated by the VP, IT
Cleanup of primary site
Re-establish primary site

Hurricane Specific Timeline

Hurricanes present a unique threat to IT. Unlike other threats to the technology infrastructure, hurricanes allow time to prepare, but due to their ability to devastate a whole region, the recovery process will be a real challenge. Our priorities will be the protection of personnel, hardware and software and maintaining communications through the main website and email.

72 Hours Prior To Landfall – The Chief Information Officer, IT shall make the determination if the probability of landfall in the Jacksonville area is high enough to initiate this plan. If it is determined that there is a high probability that Jacksonville may be impacted, the VP,IT will convene a meeting of all IT personnel. He will go over this Disaster Plan and ensure everyone understands their part in it. Distribute paper copies of the Emergency Call List (Appendix A) The Director of IT Operations will make sure the Marketing and Communications department has the appropriate VPN client software installed, a VPN login ID and password, and instructions for using the VPN connection to the AITC site. He will also ensure that appropriate personnel as determined by the VP, IT, have permissions to send emails to the Employee, Non-employee and Student Distribution Lists.

48 Hours Prior To Landfall – The Chief Information Officer, IT will evaluate the hurricane track projections and make adjustments to this plan as needed. Systems Administrators will start system backups and virtual server replication. The Manager of Networks and Telecom will verify that Physical Plant will be covering the server room windows with plywood and request fuel service for the generator. The VP,IT will coordinate with the university Disaster Preparedness Team to determine what campus buildings will require network and telephone service. Members of the IT staff will shut down switches and IPDA’s in all other buildings. The System Administrators will have the Internet connected to our switch in the AITC and test their VPN connections and logins. The System Administrators will transfer FISMO roles to the Domain Controller located at the AITC and determine if all systems are ready to go when needed. Start shutting down nonessential servers.
24 Hours Prior To Landfall - The Chief Information Officer, IT will evaluate the hurricane track projections and make adjustments to this plan as needed. Shut down remaining servers, leaving just the Domain Controllers and mail servers active (if email has not been outsourced). The PBX, voicemail and systems required for the Internet connection will not be shut down. Bring up the main JU website at the AITC and change DNS to point to it. The VP, IT will make the determination whether to station the Senior Systems Administrator at the AITC.

After The Hurricane Passes – Within 24 hours of the hurricane clearing the Jacksonville area, all IT personnel will contact their respective Directors and provide their status and location. The Directors will then provide this information to the Chief Information Officer, IT. If you are unable to contact your Director, contact the other Director or the VP, IT. The Chief Information Officer, IT will monitor conditions in the Jacksonville area to determine when it’s safe to recall personnel to implement our General Disaster Recovery Plan.

Software Safeguards

Full backups are performed at 10:00pm Friday through Saturday and Incremental backups are performed at 10:00pm Monday through Thursday to secure software and data each morning for all University Services. Every Sunday all Full backups are staged to Tape. Incremental backups are staged in the same fashion every Friday morning. Every Monday morning all staged tapes are moved to the IT safe located in the Warehouse. The backups are done on Disk and then transferred to LTO3 tapes using Commvault backup software and Brightstor Arcserve backup for Orthodontics.

Each morning the backups are checked with an e-mail log sent to the Senior Network Administrator and the Director of IT Operations.
Recovery Procedures

Central Facilities Recovery Plan

An incident that impacts IT services at the central computing/networking facilities in Founders 13 will place these plans into action. The incident may be of the magnitude that the facilities are not usable and alternate site plans are required. In this case, the alternate site portions of these plans will be implemented.

Administrative Services Recovery Plan

This portion of the disaster/recovery plan will be set into motion for Administrative Services when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode at the central site in a reasonable time.

It is assumed a disaster has occurred and the administrative recovery plan is to be put in effect. The Chief Information Officer, Information Technology, will make this decision.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

1. Determine the extent of the damage and if additional equipment and supplies are needed.
2. Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
3. Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
4. If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
5. Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
6. Notify vendor systems support personnel that help is needed immediately to begin procedures to restore systems software at JU.
7. Order any additional electrical or computer cables needed from suppliers.
8. Rush order any supplies, forms, or media that may be needed.

In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternate site:
1. Coordinate moving of equipment and support personnel into the alternate site with AITC and FTMS personnel.

2. Activate the Internet connection at CSX and change external DNS entries to point to the alternate site. (See Appendix H for specific information on this step as well as remote access.)

3. Bring the Client Services recovery materials from the off-site storage to the alternate site.

4. As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests. Virtual servers can be activated as needed.

5. Determine the priorities of the user’s software that need to be available and load these packages in order. These priorities often are a factor of the time of the month and semester when the disaster occurs. Virtual servers can be activated as needed.

6. Prepare backup materials and return these to the off-site storage area.

7. Set up Data Services operations in the alternate site.

8. Coordinate user activities to ensure the most critical jobs are being supported as needed.

9. As production begins, ensure that periodic backup procedures are being followed and materials are being placed in off-site storage.

10. Work out plans to ensure all critical Data Services support will be phased in.

11. Keep administration and users informed of the status, progress, and problems.

12. Coordinate the longer range plans with the administration, the alternate site officials, and Data Services staff for time of continuing support and ultimately the restoring of the Data Services section.

**Degraded Operations at Central Site**

In this event, it is assumed that an incident has occurred but that degraded operations can be set up in the Founders 13 Server Room. In addition to the general steps that are followed in either case, special steps need to be taken.

1. Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.

2. Replace hardware as needed to restore service to at least a degraded service.

3. Perform system installation as needed to restore service. If backup files are needed and
are not available from the on-site backup files, they will be transferred from the off-site storage.

4. Work with the various vendors, as needed, to ensure support in restoring full service.

5. Keep the administration and clients informed of the status, progress and problems.

**Academic Services Recovery Plan**

If the central site is destroyed, support of critical academic computing activities will be given from the alternate sites. Additional computer systems will be brought in as needed.

Some steps necessary in this process are listed:

1. Determine the priorities of user’s needs

2. Setup for operations support.

3. Coordinate installing additional equipment and moving support personnel.

4. When additional needed equipment is available, move backup materials from the off-site storage area.

5. Coordinate restoring any communications with Sprint, Siemens, etc.

6. Coordinate client-computing support with users.

7. As production begins, ensure that backup procedures are followed and periodic backups are stored off site.

8. Work with the Chief Information Officer, IT, the Chief Financial Officer, and users in coordinating long-range plans for restoring full support by the Academic Computing section.

**Degraded Service at Central Site**

If the central academic computing support can be resumed in a reasonable time from the central site, steps will need to be taken immediately to restore these services:

1. Determine the extent of the damage and set up procedures to bring in any needed added equipment.

2. Determine priorities of user needs and prepare for running at a degraded level of service.
3. After the hardware is functioning, perform system installation as needed. If backup files are destroyed at the central site, bring these from the off-site storage area.

4. If off-site files are used, replace these at the off-site storage as soon as possible.

5. Work with vendors as needed to ensure support is given to restore full service.

6. Keep the administration and users informed of the status, progress and problems.

**Administrative Microcomputer (PC) Recovery Plan**

Each department should have a disaster plan in place that will cover its actions in case of loss of their computer assets. Employees are encouraged to use their attached network drives for data storage. This will allow them to continue their work from any other workstation on campus or from a remote site through a VPN connection if needed. IT will coordinate the repair or replacement of damaged computers.

**Computerized Classroom/Library and Cybercafe Lab Microcomputer Recovery Plan**

Each department should have a disaster plan that will cover its actions in case of loss of their computerized classrooms. IT will coordinate the repair or replacement of damaged computers. IT maintains copies of each classroom’s computer image and will assist departments in setting up their classrooms in alternate locations. Classrooms with the FLEX system can be reconfigured quickly to host most any class. The Library and Cybercafe labs contain the FLEX system and could be used as a classroom.

The Library and Cybercafe labs are the responsibility of IT. Since each lab is in a different building, the labs can act as a back each other up in case of a casualty. IT will coordinate the repair or replacement of damaged computers.
Emergency Procedures

In case an incident has happened or is imminent that will drastically disrupt operations, the following steps should be taken to reduce the probability of personal injuries and/or limit the extent of the damage, if there is not a risk to employees. Similar steps should be followed, where appropriate.

1. An announcement should be made to evacuate the building, if appropriate, or move to a safe location in the building. As a preparation for a potential disaster, all IT personnel should be aware of the exits available.

2. If there are injured personnel, ensure their evacuations and call emergency assistance as needed.

3. If the computers and air conditioning have not automatically powered down, initiate procedures to orderly shutdown systems when possible.

4. When possible and if time is available, set up damage limiting measures.

5. Designate available personnel to initiate lockup procedures normal to last shift procedures.