Policy Name	IT Disaster Recovery Plan (DRP)
Policy Number	50000.016
Effective Date	March 29, 2019
Administrative Division	Division of Academic Affairs
Unit	Department of Information Technology
Revised Date	March 29, 2019

Table of Contents

Policy Statement

Management has approved the following policy statement:

1. Jackson State University's ("JSU" or "University") comprehensive IT Disaster Recovery Plan shall be reviewed annually.
2. A risk assessment shall be undertaken periodically to determine the requirements for the IT Disaster Recovery Plan.
3. The IT Disaster Recovery Plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key educational activities.
4. The IT Disaster Recovery Plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
5. Staff must be made aware of the IT Disaster Recovery Plan and their own respective roles.
6. The IT Disaster Recovery Plan is to be kept up to date to take into account changing circumstances.

Purpose

This document delineates JSU policies and procedures for an Information Technology Disaster Recovery Plan (referred to as "IT Disaster Recovery Plan"), as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of people, systems, and data.

Our mission is to ensure information system operation, data integrity and availability, and business continuity.

Objectives

The principal objective of the IT Disaster Recovery Plan program is to develop, test and document a well-structured and easily understood plan which will help the JSU IT department recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and educational operations. Additional objectives include the following:

- The need to ensure that employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.
- Disaster recovery capabilities are applicable to staff, vendors and others.

KEY PERSONNEL CONTACT INFORMATION

NAME AND TITLE	CONTACT OPTION	CONTACT NUMBER
Dr. Deborah Dent, Chief Information Officer (CIO) of IT	Work	601-979-4299
	Mobile	601-629-7577
	Home	N/A
	Email Address	deborah.f.dent@jsums.edu
Dr. Michael Robinson, Deputy Chief Information Officer (CIO/CTO) of IT	Work	601-979-5934
	Mobile	601-906-4985
	Home	601-878-9623
	Email Address	michael.a.robinson@jsums.edu

Mr. Philip Hairston, Director of the Office of Computing and Communications	Work	601-979-0967
	Mobile	601-331-0137
	Email Address	philip.d.hairston@jsums.edu
Mr. Umesh Remata, Manager of Communications	Work	601-979-1772
	Mobile	601-668-6799
	Email Address	umesh.r.remata@jsums.edu
Mr. Ivan Ignatius, Network Manager	Work	601-979-5962
	Mobile	601-665-8883
	Email Address	ivan.a.ignatius@jsums.edu
Mr. Gregory Anderson, Manager of Computing	Work	601-979-1845
	Mobile	601-316-8349
	Email Address	gregory.l.anderson@jsums.edu
Ms. Emily Bishop, Director of Academic IT	Work	601-979-3975
	Mobile	601-942-6458
	Email Address	emily.a.bishop@jsums.edu

EXTERNAL CONTACTS

NAME AND CONTACT	CONTACT OPTION	CONTACT NUMBER(S)
Banner- Ellucian		
Mr. Christopher Thomas	Work	601-979-1051
	Email Address	christopher.thomas@jsums.edu

1. Plan Overview

1.1 Plan Updating

It is necessary for the IT Disaster Recovery Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Department.

1.2 Plan Documentation Storage

Copies of this Plan and hard copies will be stored in secure locations to be defined by the IT Department. Each member of the IT Disaster Recovery Team will be issued a hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

1.3 Prevention

All attempts are made to prevent or limit the impact of a disaster on the information systems of our University. Specifically, the following steps have been taken:

- All servers are in a centralized and secured, locked location with access limited to technology staff and selected buildings and grounds staff.
- A separate independent cooling system is installed in the server room.
- All servers are password protected, with only select administrator level user accounts given authorization to log on.
- Uninterrupted power supplies are installed on all servers and key network equipment.

1.4 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site for mission critical applications. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site and the backup site.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Banner (ERP)	Hosted by Ellucian, no backups onsite
• Student Data Files	Hosted by Ellucian, no backups onsite
• Employee Data Files	Hosted by Ellucian, no backups onsite
• Finance & Human Resources	Hosted by Ellucian, no backups onsite
• Student Management	Hosted by Ellucian, no backups onsite
• Finance & Human Resources	Hosted by Ellucian, no backups onsite
Email	Hosted by Google, no backups onsite
Library System	On-site data storage facility
Other Critical Servers	On-site and a copy is sent off-site to a data storage facility

1.5 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal educational process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of educational disruption which could arise from each type of disaster. Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	Data Center has a draining system, sump pumps needed.
Fire	3	4	Fire and smoke detectors on all floors.
Tornado	4	3	Data Center is below ground.
Electrical storms	3	4	UPS and automatic electrical generators.
Ice Storm	3	4	
Act of terrorism	5	4	Only authorized personnel are allowed.
Act of sabotage	5	4	Only authorized personnel are allowed.
Electrical power Failure	3	3	UPS and automatic electrical generators.
Loss of communications network services	4	4	Internet connection is one route. A secondary internet connection will be implemented.

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

2. Emergency Response

2.1 Alert, escalation and plan invocation

2.1.1 Plan Triggering Events

Key trigger issues that would lead to activation of the IT Disaster Recovery Plan are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

2.1.2 Assembly Points

When the premises need to be evacuated, please refer to the Emergency Evacuation Plan (see attached).

2.1.3 Plan Invocation

When an incident occurs, the IT Disaster Recovery Plan may be implemented. All key employees must be reachable and able to activate this plan in the event of a disaster. Responsibilities are:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the university;
- Decide which elements of the disaster recovery plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

2.2 IT Disaster Recovery Team

Team members include:

- Disaster Recovery Coordinator: Chief Information Officer (CIO) - Dr. Deborah Dent
- Deputy Chief Information Officer (CIO) - Dr. Michael Robinson

Campus-Wide Recovery Team and Backups

• CIO - Dr. Deborah Dent	*Dr. Michael Robinson, Deputy CIO*
• Deputy CIO - Dr. Michael Robinson	*Artis Smith, FSO/IPSO*
• Director, Academic IT - Ms. Emily Bishop	*Kedra Taylor, Systems Integration Analyst*
• Director, Office of Computing and Communications - Mr. Philip Hairston	*Umesh Reddy and Gregory Anderson (listed below)*
• Manager of Communications Mr. Umesh Reddy	*Stevenson Paradeshi, System Administrator*
• Network Manager - Mr. Ivan Ignatius	*Roy Straughter, Wireless Network Engineer*
• Manager of Computing - Mr. Gregory Anderson	*Bennie Wade, IT Technician*

The team's responsibilities include:

- Establish facilities for an emergency level of service within 1 business day;
- Restore key services within 1 business day of the incident;
- Return to business as usual within 1 business day after the incident (depending upon incident);
- Coordinate activities with disaster recovery team, first responders, etc.

2.3 Emergency Alert, Escalation and IT Disaster Recovery Plan Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The IT Disaster Recovery Plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve smooth technology restoration.

2.3.1 Emergency Alert

The person discovering the incident calls their immediate supervisor. One of the tasks during the early stages of the emergency is to notify the IT Disaster Recovery Team that an emergency has occurred. The notification will request IT Disaster Recovery Team members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated.

2.3.2 IT Disaster Recovery Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the university's IT Disaster Recovery Plan on file in their homes in the event that the building is inaccessible, unusable, or destroyed.

2.3.3 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the university's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster. Other communication methods: radio, television, email.

2.3.4 Backup Staff

If an administrator, supervisor or staff member designated to contact other staff members is unavailable, the designated backup staff member will perform notification duties.

2.3.5 Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

3. Media

3.1 Media Contact

The President of the University, Executive Director of University Communications, or designee, will coordinate with the media.

President of the University: Dr. William Bynum, Jr.
Executive Director of University Communications: Maxine Greenleaf

3.2 Media Strategies

a. Avoiding adverse publicity
b. Take advantage of opportunities for useful publicity
c. Have answers to the following basic questions:
   - What happened?
   - How did it happen?
   - What are you going to do about it?

3.3 Rules for Dealing with Media

Only the person(s) listed in Section 3.1 above is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the individual(s) listed.

4. Insurance

As part of the university's disaster recovery strategy, any insurance claim will be handled through the Risk Management Department.

Risk Analyst: Gean Tucker

5. IT Disaster Recovery Plan Exercising

IT Disaster Recovery Plan exercises are an essential part of the plan development process. In an IT Disaster Recovery Plan exercise, no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that the emergency team is familiar with the assignment and, more importantly, is confident in their capabilities.

Successful IT Disaster Recovery Plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Upon completion of the exercises, amendments to this document may be determined necessary. Revisions to this document will be noted on the cover sheet of the IT Disaster Recovery Plan.

6. IT Disaster Recovery Kit and Supplies

An IT Disaster Recovery kit, including the following items, will be located at the MS e-Center, Jones Sampson, Hall, The Administration Tower, and other places designated by Disaster Recovery Coordinator:

- Copy of the University's IT Disaster Recovery Plan
- Copy of the telephone numbers and email addresses for all members of the IT Disaster Recovery Team.

Copy of telephone numbers with extensions and email addresses for all IT staff.

-

7. Annual Review

The Disaster Recovery Team will review and update the IT Disaster Recovery Plan annually.

Related Standards, Policies, and Processes

- IT Business Continuity Plan 50000.005

Revision History

- Created: July 10, 2015
- Revised: March 7, 2017
- Revised: February 20, 2018
- Revised: March 14, 2018
- Revised: February 13, 2019

Appendix A
Suggested Forms

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

Management of IT Disaster Recovery Activities Form

- During the IT Disaster Recovery Plan process, all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

IT Disaster Recovery Event Recording Form

- All key events that occur during the IT disaster recovery phase must be recorded.
- An event log shall be maintained by the IT Disaster Recovery Team leader.
- This event log should be started at the commencement of the emergency.
- The following event log should be completed by the IT Disaster Recovery Team leader to record all key events during disaster recovery.

Description of Disaster:
Commencement Date:
Date/Time IT Disaster Recovery Team Mobilized:

Activities Undertaken by IT Disaster Recovery Team	Date and Time	Outcome	Follow-On Action Required

IT Disaster Recovery Team's Work Completed: <Date>

IT Disaster Recovery Activity Report Form

- On completion of the initial IT disaster recovery response, the IT Disaster Recovery Team leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the IT Disaster Recovery Team together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- An IT Disaster Recovery Report will be prepared by the IT Disaster Recovery Team leader on completion of the initial IT disaster recovery response.

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the IT Disaster Recovery Team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Lessons learned

Mobilizing the IT Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the IT Disaster Recovery Team should be notified of the situation and placed on standby.
- The format shown below can be used for recording the activation of the IT Disaster Recovery Team once the work of the damage assessment and emergency response teams has been completed.

Description of Emergency:
Date Occurred:
Date Work of IT Disaster Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Communications Form

- It is very important during the IT disaster recovery activities that all affected persons and organizations are kept properly informed.
- The information given to all parties must be accurate and timely.
- In particular, any estimate of the timing to return to normal working operations should be announced with care.
- It is also very important that only authorized personnel deal with media queries.

Groups of Persons or Organizations Affected by Disruption	Persons Selected to Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Parents			
Management & Staff			
Suppliers			
Media			
IHL			
Others			

Returning Recovered Operations to Unit Leadership

- Once normal operations have been restored, it will be necessary to return the responsibility for specific operations to the original department.
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to normal operations-as-usual