



| | |
|-------------------------|--------------------------------------|
| Policy Name | Business Continuity Plan (BCP) |
| Policy Number | 50000.005 |
| Effective Date | March 29, 2019 |
| Administrative Division | Division of Academic Affairs |
| Unit | Department of Information Technology |
| Revised Date | February 11, 2022 |

Please Note: Managers must keep a copy of this document at home. These documents have to be kept in an easily accessible place in case of emergency.

| | |
|--|----------|
| Table of Contents | 1 |
| Introduction | 1 |
| Priorities and Responsibilities | 1-2 |
| Key Risks and Minimization Measures | 2-3 |
| a. Assumptions | 2 |
| b. Disaster Events | 2 |
| c. Loss of Technology | 2 |
| Roles and Responsibilities | 3 |
| Business Continuity Plans | 3-6 |
| Emergency Delegations List | 6 |
| Related Standards, Policies, and Processes | 6 |
| Revision History | 6 |

I. Overview

This business continuity plan has been developed to minimize disruption to Jackson State University (JSU) IT services in times of crisis. It lays out what the business should do if normal business activities cannot be continued due to a disabling event such as loss of technology, the building or a large proportion of staff is without services to assist JSU business processes.

The business continuity plan:

- Realistically formalizes the action you will need to take.
- Minimize the downtime for the business.
- Identifies business priorities so that if services are limited, they can be allocated effectively.

II. Priorities and Responsibilities

During an emergency these are the priorities and responsibilities for Jackson State University.

| | |
|---------|--|
| General | <p>All JSU staff are safe and accounted for.</p> <p>JSU manages the situation by ensuring that:</p> <ul style="list-style-type: none"> • Managers or others notify the Chief Information Officer (CIO) of IT immediately of business interruption issues. • Staff actions and priorities are consistent with overall business recovery strategy. • There are manual workarounds for critical business processes. • The public can be provided with fundamental services at an appropriate level. |
|---------|--|

| | |
|----------------------------|--|
| Critical business function | <p>Critical business functions of JSU:</p> <ul style="list-style-type: none"> Communications <ul style="list-style-type: none"> Ensure travelling staff know the extent of the emergency and have a contact number for JSU's office. Establish what electronic systems are available and set up for use. Ascertain what business functions need to be provided. |
|----------------------------|--|

III. Key Risks and Minimization Measures

a. Assumptions

JSU's IT Department operates from two main locations, it is possible that the whole of Jackson State's core business could be disrupted. Business support system failure could disrupt business, but the assumption is that serious disruption is not likely to occur until at least after 24 hours. The business continuity plan takes this into account.

b. Disaster Events

This plan concentrates on the events that are most likely to occur. These three events (in order of impact) are:

1. Loss of technology:
 - a. Payroll
 - b. Email
 - c. Network (including file and print) and remote access
 - d. Phones – landlines
 - e. CBORD
 - f. Financial system- Banner/Touchnet
 - g. Website
 - h. Loss of building/functions

The graph below shows what tolerable time frames of loss are in the event a disaster occurs.

c. Loss of Technology

| System | Tolerable outage | Tolerable data loss |
|-----------------------------------|------------------|---------------------|
| Payroll | 8 hours | 8 hours |
| Email | 4 hours | 4 hours |
| Network (including remote access) | 4 hours | 4 hours |
| File server/sharing | 4 hours | 4 hours |
| Phones (landline) | 4 hours | 4 hours |
| CBORD | 4 hours | 4 hours |
| Financial system- Banner/Touchnet | 4 hours | 4 hours |
| Website | 4 hours | 4 hours |

IV. Roles and Responsibilities

During an emergency these are the roles and responsibilities.

| Role | Who | Responsibilities |
|---|------------------|---|
| Chief Information Officer (CIO) of Information Technology | Dr. Deborah Dent | <p>Contacting the AVP at first knowledge of an emergency</p> <p>Arranging the initial meeting of the Emergency Decision Group (EMT, CSIRT and Risk Analyst) to:</p> <ul style="list-style-type: none"> activate the Business Continuity Plan |

| | | |
|--|--|--|
| | | <ul style="list-style-type: none"> undertake emergency tasks Confirm critical business functions and business recovery location Reinstating services at JSU |
| Deputy Chief Information Officer (CIO) of Information Technology | Dr. Michael Robinson | Contacting the VP at first knowledge of an emergency Ratifying the decisions of the Emergency Decision Group Communicating to the organization (including the President's Cabinet / Security Advisory Board if applicable) |
| Emergency Management Team (EMT) | Dr. Charlotte N Crisler Public Safety, Risk manager | Coordinate the setting-up of the business recovery office along with the managers. |
| Cybersecurity Incident Response Team (CSIRT) | See Appendix A | Coordinate the management of BCP, DRP, IRP |
| University Communications/Public Relations Officer | Alonda Thomas / Chief Communications Officer and Associate Vice President for Marketing and Communications | Communicating with: <ul style="list-style-type: none"> clients stakeholders media anyone else important to JSU and other relevant organizations |

V. Business Continuity Plans

a. Payroll

| Core business functions | Characteristics of interruption | Short term (Up to 4 hours) | Long term (More than 24 hours) |
|-------------------------|--|--|---|
| Payroll | No access to building & no access Payroll system. | Arrange with Bank Plus to process the same payments as the previous pay run. | CSIRT to arrange for Payroll software & backups to be installed on a standalone PC. |
| | Access to building but no access to Payroll system | Arrange with Bank Plus to process the same payments as the previous pay run. | CSIRT to arrange for Payroll software & backups to be installed on an alternative PC. |

b. Email

| Core business functions | Characteristics of interruption | Short/Long Term- 4/24 hrs |
|-------------------------|--|---|
| Delivery of email | No access to building and Google server down | We are hosted so we submit tickets to Google. |

c. Network (including file, print, and remote access)

| Core business functions | Characteristics of interruption | Short term (Up to 4 hours) | Long term (More than 24 hours) |
|-------------------------------|--|--|--------------------------------|
| General business applications | No access to building but servers operating. | CSIRT contacts all IT suppliers. IT provide support remotely. IT assist staff to access network remotely. | Work offsite. |

| | | | |
|--------------------------------------|--|---|--|
| | | | Temporary IT systems will be arranged at business recovery office if necessary. |
| General business applications | No access to building and Terminal Server not running. There will be no access to shared drives, print services or CBORD/specialist applications. | CSIRT contacts suppliers. IT provide support remotely. If the server cannot be fixed remotely there is no access to shared drives, print services, or specialist applications. | The implementation or repair of the Terminal Server will have to wait until access to the building has been restored. If all servers are running except the Terminal Server, at some stage a decision may be made to purchase & setup all the services at the business recovery office. |
| General business applications | Access to building but Terminal Server not running. There will be no access to shared drives, print services or CBORD/specialist applications. | CSIRT to contact IT suppliers to attempt repair of server. Until the server can be fixed or replaced, configure the standby server to run terminal services (gives access to shared drives, print services or CBORD/specialist applications), printing & backups. Limited shared drives may be made available. IT assist staff to access the new configuration. | If the Terminal Server is unrepairable, purchase a new server. Implement the new/repared Terminal Server. |

d. Phones – Landlines

| Core business functions | Characteristics of interruption | Short term (Up to 4 hours) | Long term (More than 24 hours) |
|--------------------------------|---|---|--|
| Phone calls | No access to building and phone system down | Contact ATT HVS and phone system suppliers. Phone system suppliers to attempt remote repair but unlikely as phone system must be running for remote access to work. Arrange for the ATT HVS to setup diversions of main number (includes all DID's AND DOD's) to a mobile phone or to a landline in the business recovery office. | If phone system is unrepairable, purchase a new system. The implementation or repair of the phone system will have to wait until access to the building has been restored. Arrange for ATT HVS to remove the phone diversions. |
| | Access to building but phone system down | Contact ATT HVS and phone system suppliers. Phone system suppliers to attempt repair. In the meantime, calls will automatically divert to the mobile phones on file. Install a temporary phone system. | If phone system is unrepairable, purchase a new system. Implement the new/repared phone system. Arrange for ATT HVS to remove the phone diversions. |

e. Website

| Core business functions | Characteristics of interruption | Short term (Up to 4 hours) | Long term (More than 24 hours) |
|-------------------------|---------------------------------|---|---|
| Website | Website not working | The University Webmaster will contact website supplier (Pantheon). Webmaster and website supplier (Pantheon) to assist with the repair of the JSU website. | If website is unrepairable, work with current or new suppliers to recreate website from backups or redevelop. |

VI. Emergency Delegations List (if applicable)

Delegations will be sought to ensure emergency expenditure can be approved by:

| Position | Level of Authority |
|-------------------------------|--------------------|
| President of the University | \$50,000 and above |
| Provost | \$50,000 and below |
| Chief Financial Officer (CFO) | \$+ or – 50,000 |

Related Standards, Policies, and Processes

- IT Disaster Recovery Plan 50000.015

Revision History

- Initial Draft: March 7, 2017
- Revised sections 1-4: February 8, 2018
- Revised entire document: February 13, 2018
- Revised March 29, 2019
- Revised and updated Emergency Manager and Communications February 11, 2022

