



Emergency Recovery Plan

Version 0.3 – June 2022

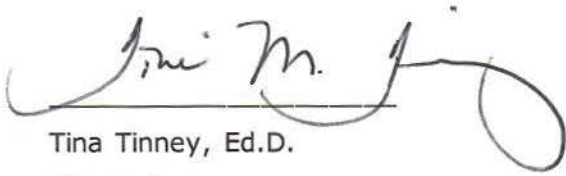
Nunez Community College
3710 Paris Road, Chalmette, LA 70043

Telephone: (504) 278-6203

Fax: (504) 278-6480

Authorization

This plan has been prepared in accordance with the Nunez Community College Risk Management Policy and is authorized by the Chancellor.

A handwritten signature in black ink, appearing to read "Tina M. Tinney", written over a horizontal line. The signature is cursive and includes a large loop at the end.

Tina Tinney, Ed.D.

Chancellor

Distribution

The electronic distribution of this plan to Nunez Community College recipients is controlled by the Chancellor.

Title	Office Location
Vice Chancellor of Education, Training, and Student Success	Admin 2 nd Floor
Assistant Vice Chancellor of Education, Training, and Student Success	Kane Technology Bldg. 1 st Floor
Associate Vice Chancellor of Advancement and External Affairs	Admin 1 st Floor
Interim Executive Director of Strategic Engagement and Human Capital	Admin 2 nd Floor
Chief Financial Officer	Admin 2 nd Floor
Director of Accounting and Budget	Admin 2 nd Floor
Director of Communications	Admin 2 nd Floor
Dean of Strategic Enrollment and Student Success	Admin 1 st Floor
Director of Information Technology	AST 2 nd Floor
Director of Facilities Management	Facilities Bldg. 1 st Floor
Dean of Instruction	AST 2 nd Floor
Dean of Nursing and Allied Health	Bldg. D 2 nd Floor

Table of Contents

AUTHORIZATION	2
AMENDMENTS	3
DISTRIBUTION	4
GLOSSARY	8
PART ONE – ACTIVATE THIS PLAN	10
1.1. AUTHORITY TO ACTIVATE THIS PLAN.....	10
1.2. MEDIA RESPONSE.....	10
1.3. DOCUMENT REFERENCES.....	10
PART TWO – OVERVIEW AND SCOPE	11
2.1. OVERVIEW.....	11
2.2. AIM.....	11
2.3. OBJECTIVES.....	11
2.4. RECOVERY TIME REQUIREMENTS.....	12
2.5. SCOPE.....	13
PART THREE – ORGANIZATION	14
3.1. THE CRISIS MANAGEMENT TEAM.....	14
3.2. MANAGEMENT TEAM.....	15
3.3. RECOVERY TEAM.....	16
3.4. FACILITY TEAM.....	17
PART FOUR – ROLES AND RESPONSIBILITIES	18
4.1. MANAGEMENT TEAM.....	18
4.2. RECOVERY TEAM.....	19
4.3. FACILITY TEAM.....	20
PART FIVE – PROCESSES	21
5.1. RECOVERY STRATEGY.....	21
5.2. BUSINESS RESUMPTION.....	22
5.3. MAINTAIN ERP DOCUMENTATION.....	24
5.4. COMMAND CENTER OPERATIONS.....	25
PART SIX – PROCEDURES	26
6.1. MANAGEMENT TEAM.....	26
6.2. FACILITY TEAM.....	28
6.3. RECOVERY TEAM.....	30
APPENDIX A – CONTACT LIST	32
NUNEZ COMMUNITY COLLEGE MANAGEMENT.....	32
FACILITY TEAM.....	32
RECOVERY TEAM.....	33
DISASTER RECOVERY / SALVAGE VENDORS.....	33

KEY VENDOR CONTACT.....	33
KEY STAKEHOLDER CONTACTS.....	34
SYSTEM CONTACTS.....	34
APPENDIX B – SYSTEM RECOVERY REQUIREMENTS.....	35
RECOVERY PRIORITY FOR IT SYSTEMS	35
APPENDIX C – RETRIEVAL OF OFF-SITE BACKUPS.....	36
INTRODUCTION.....	36
PROCEDURE.....	36
APPENDIX D – SYSTEM NOTIFICATION.....	37
NOTIFY LOUISIANA COMMUNITY AND TECHNICAL COLLEGE SYSTEM (LCTCS) OF DISASTER.....	37
CONTACT PROCEDURES:	37
APPENDIX E – BUSINESS IMPACT ANALYSIS PROCESS	38
PROCESS.....	38
OUTCOMES	38
WHOLE OF BUSINESS APPROACH.....	38
FREQUENCY.....	38
APPENDIX F – COMMAND CENTER DETAILS	39
COMMAND CENTER LOCATIONS.....	39
COMMAND CENTER CHECKLIST	39
RESOURCE CHECKLIST.....	41
APPENDIX G – IT RECOVERY PROCEDURES	42
<u>IT DISASTER RECOVERY PLAN</u>	42
APPENDIX I – MEDIA CRISIS MANAGEMENT	53
PROCEDURES FOR DEALING WITH THE MEDIA.....	53
APPENDIX J – EVENT LOG	54

Table of Figures

Figure 1: Recovery Time Requirements12

Figure 2: Crisis Management Team14

Figure 3: Management Team Organization15

Figure 4: Recovery Team Organization16

Figure 5: Facility Team Organization17

Figure 6: Disaster Recovery Strategy Overview21

Figure 7: Business Resumption Process23

Figure 8: Maintain ERP Documentation Activities24

Figure 9: Command CENTER Activities25

Figure 10: Management Team Activities26

Figure 11: Facility Team Action Process.....28

Figure 12: Recovery Team Activities30

Glossary

ACTIVATION: The implementation of disaster recovery capabilities, procedures, activities, and plans in response to an emergency or disaster declaration; the execution of the recovery plan.

ALERT: Notification that a potential disaster situation exists or has occurred; direction for the recipient to stand by for possible activation of the Disaster Recovery Plan.

ALTERNATE SITE: An alternate operating location to be used by business functions when the primary facilities are inaccessible. 1) Another location, computer CENTER or work area designated for recovery. 2) Location, other than the primary facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster. **SIMILAR TERMS:** Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility, Backup Location, Recovery Site, and Recovery CENTER.

ALTERNATE WORK AREA: Office recovery environment complete with office infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.); also referred to as Work Space or Alternative Work Site.

APPLICATION RECOVERY: The component of Disaster Recovery that deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced.

BACKUP GENERATOR: An independent source of power, usually fueled by diesel (sometimes natural Gas).

DISASTER RECOVERY PLANNING (ERP): Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption. **SIMILAR TERMS:** Emergency Planning, Recovery Planning.

EMERGENCY RECOVERY PROGRAM: An ongoing program supported and funded by executive staff to ensure emergency recovery requirements are assessed, resources are allocated, and recovery and emergency strategies and procedures are completed and tested.

COLD SITE: An alternate facility that already has the environmental infrastructure in place required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, communications network, etc. These must be provisioned at time of disaster.

COMMAND CENTER: Facility separate from the main facility and equipped with adequate communications equipment from which initial recovery efforts are manned and media-business communications are maintained. The management team uses this facility temporarily to begin coordinating the recovery process until the alternate sites are functional.

CONTACT LIST: A list of team members and/or key players to be contacted. (Mobile Number, Home Number, Pager, etc.)

CRISIS MANAGEMENT TEAM: A crisis management team will consist of key executives as well as key role players (i.e., media representatives, legal counsel, facilities manager, disaster recovery coordinator, etc.) and the appropriate owners of critical organization functions.

DAMAGE ASSESSMENT: The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.

DECLARATION: A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred, and that triggers pre-arranged mitigating actions (e.g., move to an alternate site).

DISASTER: A sudden, unplanned catastrophic event causing great damage or loss. Any event that causes an organization to be unable to provide critical business functions for a pre-determined period of time.

DISASTER RECOVERY: Activities and programs designed to return Nunez Community College operations to an acceptable condition. 1) The ability to respond to an interruption in services by implementing a disaster recovery plan to restore Nunez Community College critical business functions.

DISASTER RECOVERY PLAN: The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business disruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

EMERGENCY: A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.

HOT SITE: An alternate facility that already has the computer, communications and environmental infrastructure in place that is required to recover critical business functions or information systems.

MAXIMUM TOLERABLE OUTAGE (MTO): The maximum tolerable outage is the amount of time the critical business functions may be without the support of IT systems and applications before business operations are severely impacted. The MTO encompasses all activities from point of impact to point of recovery.

OFF-SITE STORAGE: Alternate facility, other than the primary production site, where duplicate vital records and documentation may be stored for use during disaster recovery.

RECOVERY POINT OBJECTIVE (RPO): The point in time to which systems and data must be recovered after an outage (e.g., end of the previous day's processing). RPOs are often used as the basis for the development of backup strategies.

RECOVERY TIME OBJECTIVE (RTO): The period of time within which systems, applications or functions must be recovered after a disaster declaration (e.g., one business day). RTOs are often used to determine whether or not to implement the recovery strategies/plan.

WARM SITE: An alternate processing site which is equipped with some hardware, and communication interfaces, electrical and environmental infrastructure which is only capable of providing backup after additional provisioning, additional software, or modifications.

PART ONE – ACTIVATE THIS PLAN

To activate this plan in the event of a real disaster, turn to PART SIX (Procedures)

1.1. Authority to Activate this Plan

The Chancellor has the **exclusive** authority to activate this plan by process of declaring a disaster. If this person is unavailable, the Chief Financial Officer may also declare a disaster.

The Chancellor will assume the role of Crisis Management Team Leader, and the associated responsibilities. The Chancellor may delegate the Crisis Management Team Leader role, or if the Chancellor is unavailable, the Chief Financial Officer may assume the Crisis Management Team Leader Role. See PART THREE – ORGANIZATION

1.2. Media Response

It should be noted that Nunez Community College staff must follow the *Media Crisis Management Procedure for Dealing with the Media*. – See APPENDIX I – MEDIA CRISIS MANAGEMENT

1.3. Document References

Description	Location
Emergency Evacuation Procedures	Director of Facilities Management – Facilities Bldg
Risk Management Policy	Director of Facilities Management – Facilities Bldg
Employee Handbook	Interim Executive Director of Strategic Engagement and Human Capital – Admin Bldg
IT Disaster Preparedness and Recovery	Director of Information Technology – AST Bldg

PART TWO – OVERVIEW AND SCOPE

2.1. Overview

A disaster is an event that significantly reduces Nunez Community College ability to provide normal services to its clients. Typically, an outage to the Nunez Community College core processes and systems exceeding 24 hours is deemed to be a disaster; however, when an event occurs greatly affects the level of impact to Nunez Community College operations.

This plan details the communications structure, role and responsibilities of the Crisis Management Team (CMT).

The CMT is responsible for managing the rapid and orderly resumption of Nunez Community College core processing; consequently, the members of the CMT have the appropriate authority and skills to accomplish their assigned tasks.

IT hardware and software problems, while they might in some instances be significant, will be resolved through normal problem resolution methods. The typical disaster involves an unscheduled event that causes the primary site (production site) to be inaccessible for an indefinite period of time. A disaster declaration begins the formal disaster recovery process described in this section.

2.2. Aim

The aim of this plan is to set out the mitigation, preparation, warning, response and business continuity arrangements for the Nunez Community College core processes and environment which are supported from the Nunez Community College campus in Chalmette, LA.

2.3. Objectives

The objective is to provide for restoration and continuation of Nunez Community College core processes and environment when a disaster occurs. This is accomplished by developing and maintaining a detailed Emergency Recovery Plan (ERP) that will organize and govern a disaster recovery operation. The ERP must:

- provide the information and procedures necessary to respond to an occurrence, notify personnel, assemble recovery teams, recover data and resume processing at the current or alternate site as soon as possible after a disaster has been declared
- create a disaster recovery structure strong enough to provide guidance to all interrelated groups, yet flexible enough to allow Nunez Community College personnel to respond to whatever type of disaster may occur
- provide specific action plans for each functional area
- identify those activities necessary to resume full services at the reconstructed disaster site or new permanent facility
- establish a return to a business as usual environment.

Note: Availability of backup data is critical to the success of disaster recovery. Backup and restore processes that include scheduling tape management, off-site storage, and data restorations are day-to-day processes covered in operating procedures manuals. Good practices are assumed, as are the availability of backup media that can be readily restored.

2.4. Recovery Time Requirements

The following requirements are a result of the Business Impact Analysis process, which forms part of the Nunez Community College emergency recovery program:

- **Maximum Tolerable Outage (MTO).** The maximum tolerable outage is the amount of time Nunez Community College critical business functions may be unavailable before Nunez Community College business operations are severely impacted. The MTO encompasses all activities from point of impact to point of recovery completion as described in SECTION 5.1 Recovery Strategy.
- **Recovery Time Objective (RTO).** The Recovery Time Objective is the time taken to recover the in-scope services for Nunez Community College from disaster declaration to the point where the infrastructure is handed over to the Nunez Community College business teams. The RTO for Nunez Community College is 72 Hours.
- **Recovery Point Objective (RPO).** The recovery point objective is the worst data loss that the Nunez Community College is willing to accept. In other words, this is the point from which recovery of lost data must take place. The RPO for Nunez Community College is 24 Hours.

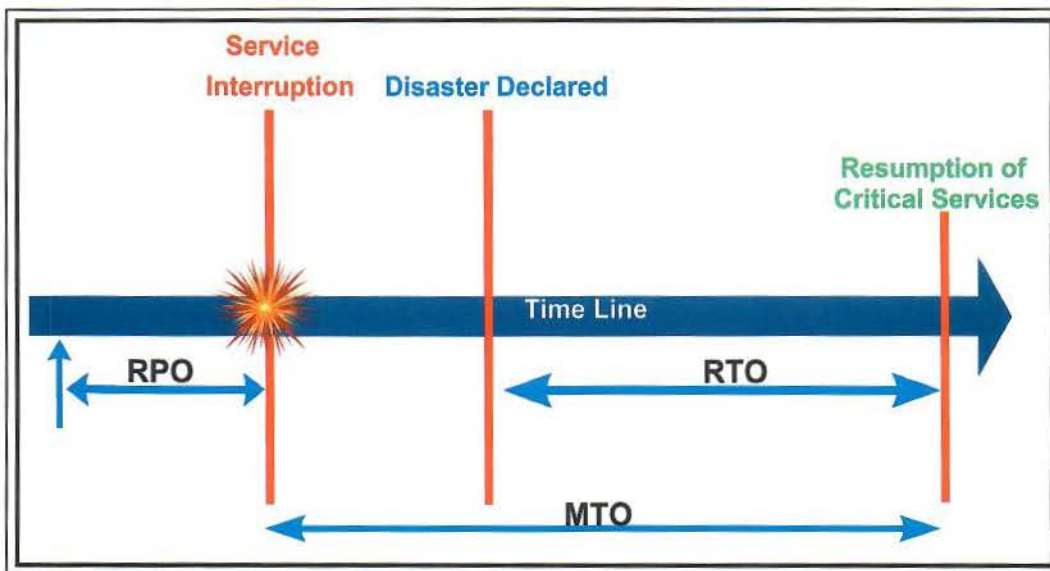


Figure 1: Recovery Time Requirements

2.5. Scope

2.5.1. Scope of Recovery

This plan is devised to address a significant outage of Nunez Community College core processes at the Chalmette campus and will therefore cover the following:

- 1. Academics**
- 2. Student Services**
- 3. Business Affairs**
- 4. Facilities**
- 5. Information Technology**
- 6. Human Resources**
- 7. External Affairs/Media Relations (PR)**

2.5.2. Exclusions

- This ERP does not address the recovery of Nunez Community College business operations during a disaster, such as manual fallback procedures, resynchronization of business processes and applications. Responsibility for this resides with the relevant groups within the College.
- Any development or test environments.
- Any disaster affecting an area greater than the Chalmette campus (i.e., metropolitan area).

2.5.3. Recovery Validation

- System Health Checks performed by relevant Nunez Community College technical services.
- Validation checks performed by business representatives.

2.5.4. General Exclusions

- A disaster of such a magnitude that there are not enough personnel to resource the recovery in order to meet Nunez Community College objectives.

PART THREE – ORGANIZATION

3.1. The Crisis Management Team.

The Crisis Management Team (CMT) includes 3 sub-teams responsible for the successful execution of the Disaster Recovery Plan. These teams are:

- **The Management Team** — responsible for managing the recovery, and communicating with vendors, key clients, stakeholders and Nunez Community College senior management. This team is also responsible for the on-going recovery program and for keeping this plan current during a disaster.
- **The Recovery Team** — responsible for restoring computing services at alternate facilities. The Recovery Team will also restore computing service at the restored original facilities, if available.
- **The Facility Team** — responsible for damage assessment, damage mitigation, salvage, and physical restoration of the office environment.

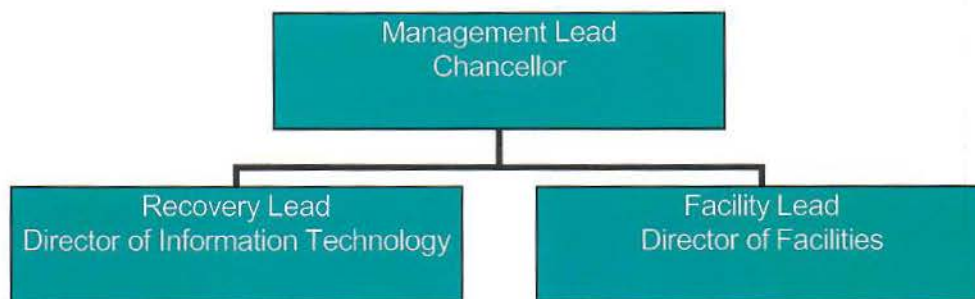


Figure 2: Crisis Management Team

3.2. Management Team

The Management Team (Figure 3) is responsible for deciding on the course of action and coordinating all activities during the recovery period. Table 1 (page 17) shows the kinds of skills and authority levels needed for Management Team membership.

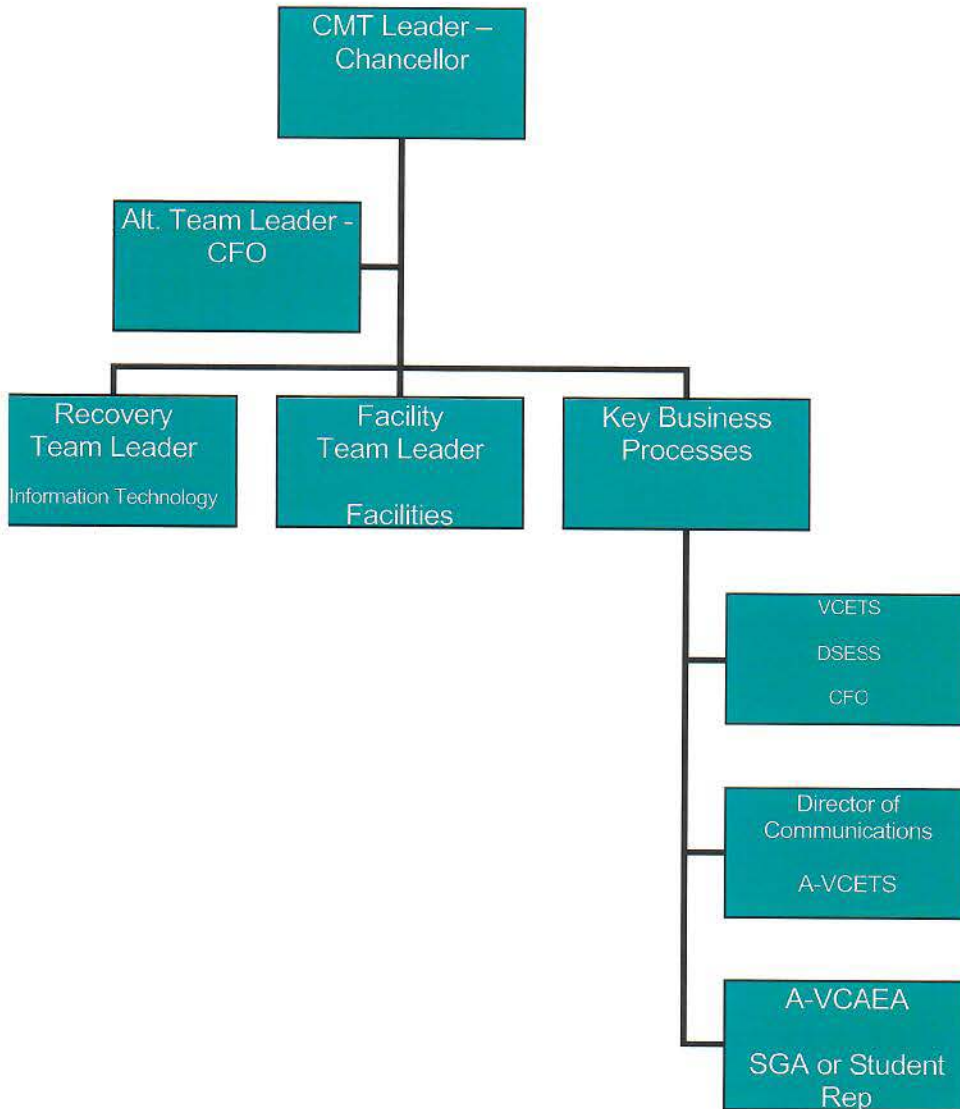


Figure 3: Management Team Organization

3.3. Recovery Team

The purpose of the Recovery Team is to establish operations at an alternate-processing site or restore services at the disaster site. The skills needed by this team are all the skills normally used in Nunez Community College production work, as shown in Table 2 (page 18).

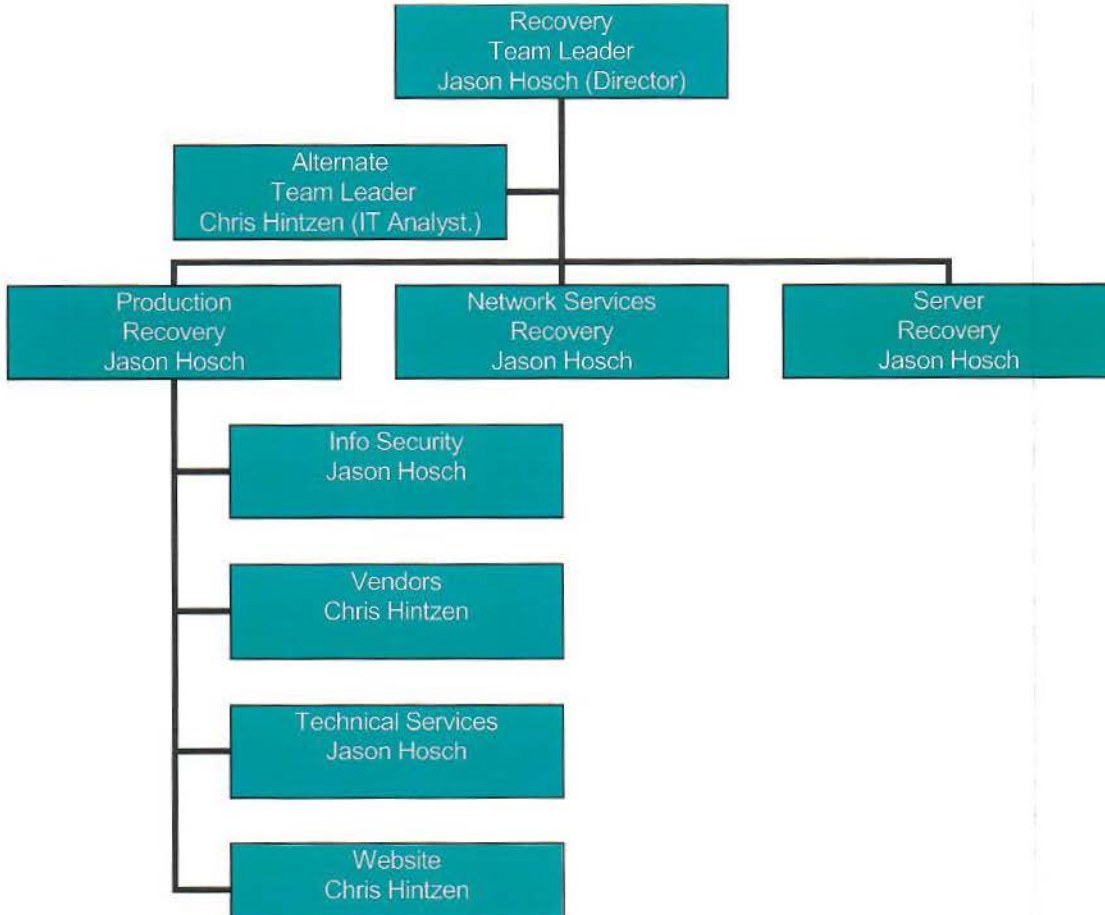


Figure 4: Recovery Team Organization

3.4. Facility Team

The purpose of this team is to secure, salvage, and restore the primary site to operational status as quickly as possible. The team may also be needed to prepare an alternate facility for occupation. The skills required of team members include knowledge of computing and network hardware. The Facility Team leader is also a member of the management team. Table 3 (page 19) shows the kinds of skills and authority levels needed for Facility Team membership.

The Facilities Team is tasked with conducting an in-depth damage assessment with recommendations to management on required repair or restoration activities. Concurrent with performing their evaluation procedures, members are responsible for initiating and monitoring recovery tasks assigned to their functional areas. Each team has its own chapter of detailed instructions later in this plan.

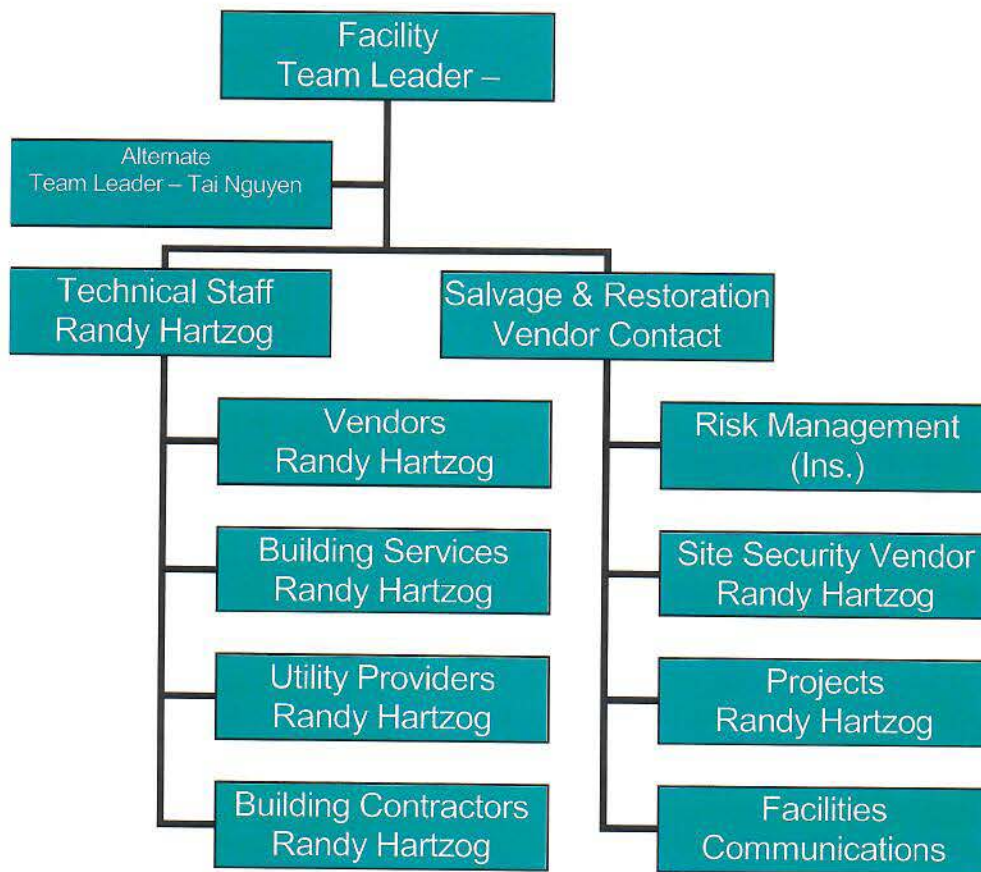


Figure 5: Facility Team Organization

PART FOUR – ROLES AND RESPONSIBILITIES

4.1. Management Team

Management Team roles and responsibilities are summarized in Table 1.

Team Member	Role/Responsibility
Crisis Management Team Leader	Senior manager to oversee recovery. Authority to declare a disaster. Chancellor.
Alternate Mgmt. Team Leader	Full authority to act if Team Leader is not available. Chief Financial Officer
Facility Team Leader	Oversee facility, security, damage assessment, salvage and reconstruction. Director of Facilities Management.
Recovery Team Leader	Knowledge of computer operations, systems, networks. Director of Information Technology.
Manager, Finance	Contact regulatory authority as soon as possible. Authority to spend the amounts required to fund recovery in the first days. Chief Financial Officer
Manager, Communications	Authority to speak for the organization. Director of Communications.
Corporate Legal	Ability and authority to make legal/contractual decisions. Chief Financial Officer
Manager, Human Resources	Knowledge and authority to make Human Resources decisions. Interim Executive Director of Strategic Engagement and Human Capital via Appointing Authority.

Table 1: Management Team Roles/Responsibilities

4.2. Recovery Team

Recovery Team roles and responsibilities are summarized in Table 2.

Team Member Titles	Responsibility
Recovery Team Leader	Senior Manager, knowledgeable of computer operations, systems, etc. Director of Information Technology. <ul style="list-style-type: none"> • Establish the command CENTER, as described in section 5.4. • Advise the alternate site of a disaster alert prior to a disaster being declared. • Advise the alternate site of a declared disaster. • Advise the alternate site of a stand down from alert if recovery is not to be effected at the site or the disaster is not declared. • Liaise with alternate site management and personnel
Alternate Team Leader	Full authority to act if team leader is not available. Information Technology Analyst.
Production Operations Recovery	Restoration of operations, services, security and change management services and technical services. Information Technology Analyst.
Network Services Recovery	Recovery of network infrastructure. Includes recovery of hardware components, connectivity to the recovery site and recovery of critical network software. Director of Information Technology
Server Recovery	Recovery of critical servers. Director of Information Technology

Table 2: Recovery Team Roles/Responsibilities

4.3. Facility Team

Facility Team roles and responsibilities are summarized in Table 3.

Team Member Titles	Responsibility
Facility Team Leader	Authority and knowledge to deal with damage assessment, damage mitigation, salvage, restoration, alternate site installation, etc. Director of Facilities Management
Alt. Facility Team Leader	Authority and knowledge to act in place of the team leader. CFO.
Hardware Experts	As required, depending upon the situation. (See Figure 5).
Technical Staff Members	Will be sourced from the Nunez Community College personnel pool to assist with salvage, restoration, etc. (See Figure 5).
Vendors (Site, Hardware, Maintenance, Communications, Salvage/Restoration)	IT Support is a critical element in the Facility Team. Much of the team effort is in coordinating, supporting, and reporting on recovery activities. (See Figure 5).

Table 3: Facility Team Roles/Responsibilities

PART FIVE – PROCESSES

5.1. Recovery Strategy

Following the occurrence of a suspected disaster, there are **three** processes that will take place prior to the activation of the actual recovery process:

- **Disaster Alert Notification** – to notify CMT members, recovery teams, and the offsite media storage provider that a disaster may have occurred or is evolving.
- **Damage Assessment** – to ascertain whether a disaster has occurred, assess the extent of the damage, and to assemble the recovery teams if necessary.
- **Disaster Declaration Assessment** – to ascertain if the predetermined MTO is likely to be compromised and that invoking the ERP and its associated procedures is necessary.

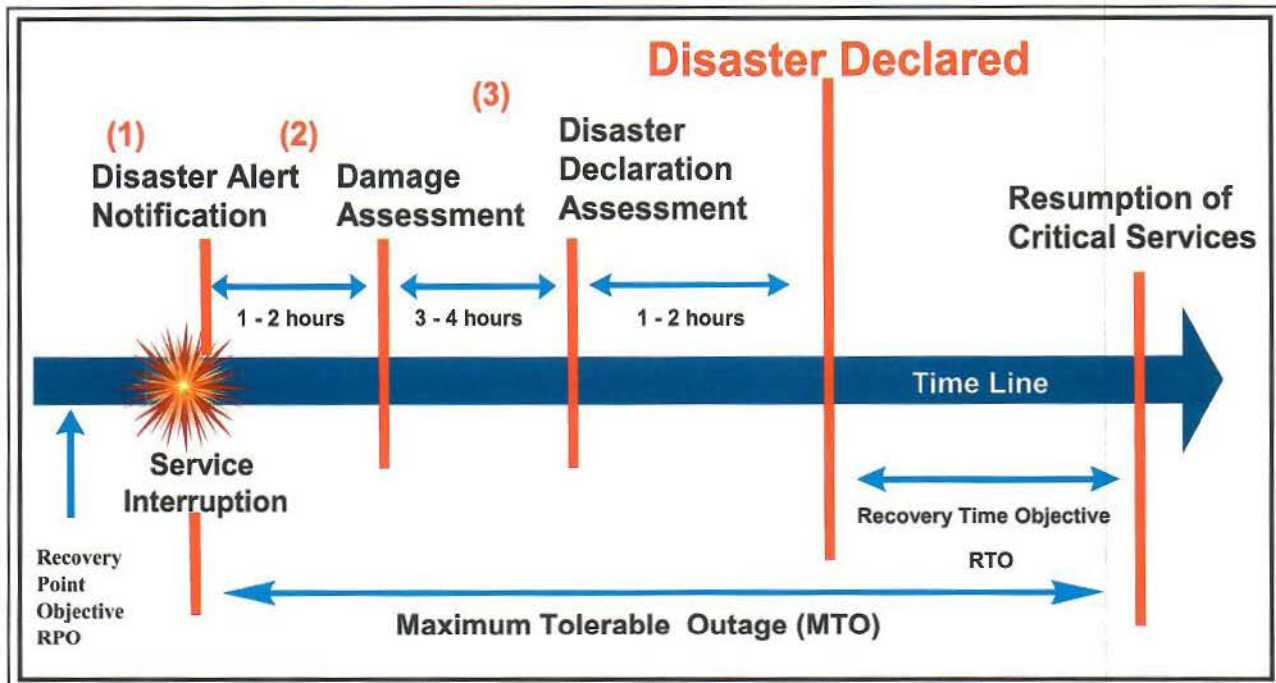


Figure 6: Disaster Recovery Strategy Overview

If there is a major incident where the damage is not widespread and the Chalmette campus is not seriously affected, it may not be obvious to the person(s) who detected such an incident whether it constitutes a disaster, especially when the damage is confined and local. Where possible, it is expected that the usual problem management procedures be followed in dealing with such incidents.

5.2. Business Resumption

This section provides the approach to restoring the Chalmette campus (disaster site) or establishing a new primary site. The extent and timing of the recovery activities will vary depending upon the nature of the disaster. These activities will need to be coordinated and planned as a parallel stream to establish stable production operations at the recovery site. Detailed activities are contained in the Procedures section of this document.

The decision concerning the approach to re-establishing the Chalmette campus site and secondary sites should be made as soon as practically possible after a disaster occurs. This allows all the affected areas to adapt their procedures and staffing according to the expected length of the outage. The alternatives to be considered are:

1. The Chalmette campus site is to be restored to original operating status. This will require the establishment of new technical infrastructure according to current requirements and specifications.
2. The Chalmette campus site is to be upgraded to preferred level of operating status. This will require:
 - establishment of new technical infrastructure according to revised requirements
 - establishment of new facilities and services according to revised requirements.
3. A new primary site is chosen. This will require:
 - assessment and risk analysis of the new site for suitability
 - new arrangements with suppliers and service teams to be established; i.e., for off-site tape collections and deliveries
 - establishment of new technical infrastructure according to current requirements and specifications.
4. The secondary site is to become the new production site. This will require:
 - communications, floor space and other facilities to be upgraded to be commensurate with the original production site
 - a new secondary site to be established
 - assessment and risk analysis of the new site for suitability
 - new arrangements with suppliers and service teams to be established; i.e., for off-site tape collections and deliveries
 - establishment of new technical infrastructure according to current requirements and specifications.

5.2.1. Business Resumption Process

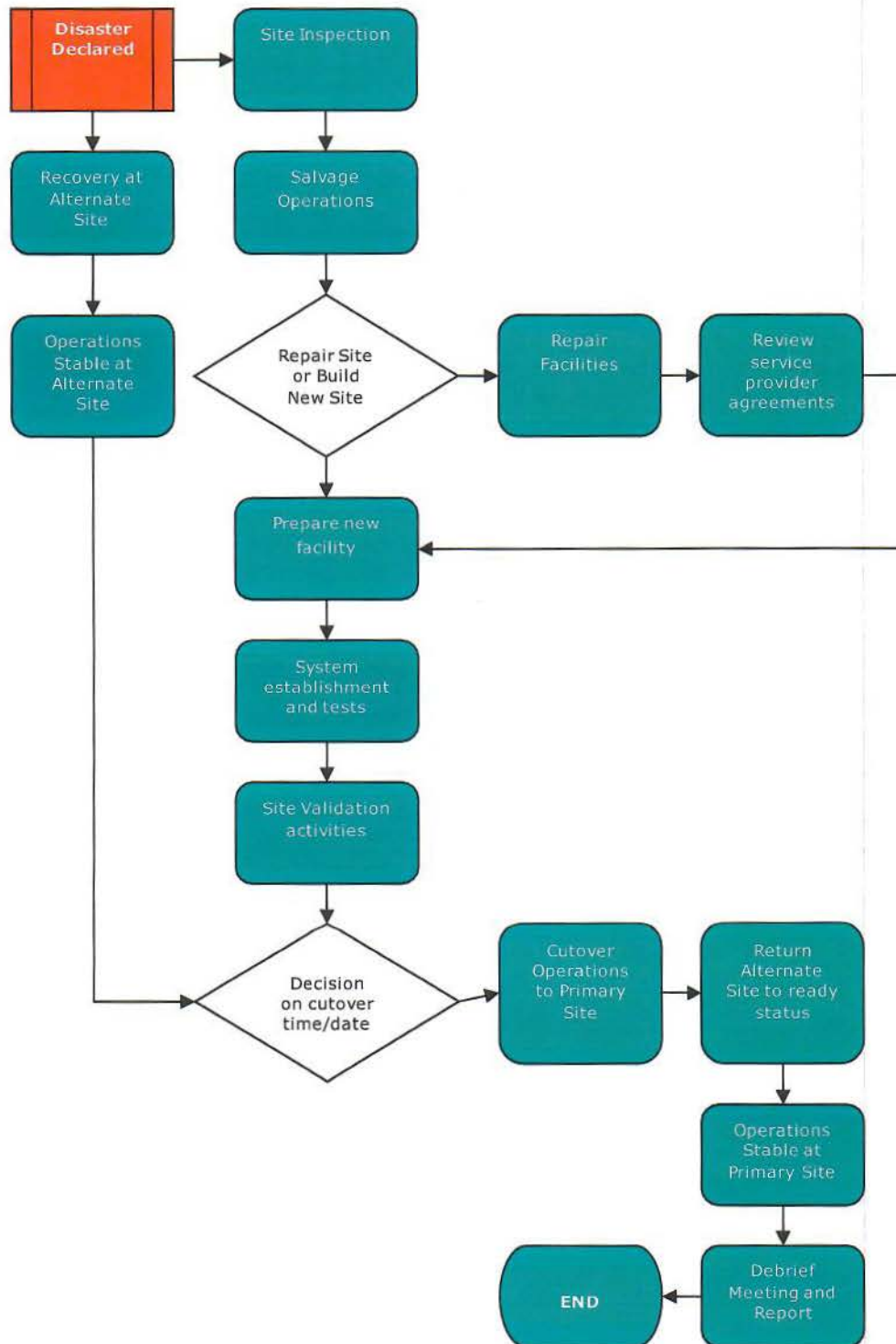


Figure 7: Business Resumption Process

5.2.2. Debriefing

Prior to closure of a disastrous situation and standing down of the Crisis Management Teams, a debriefing of all participants should be conducted. A debriefing will ensure that:

- all required recovery and normal business resumption tasks have been performed
- ongoing system, business and client impacts are being addressed
- Nunez Community College can ascertain and understand the cause, nature and impact of the disaster on the organization
- financial impacts are clearly identified and documented for insurance claims
- lessons learned are clearly identified and incorporated into a knowledge database for future ERP development and disaster management
- deficiencies in the current process are clearly identified in way that projects can be established to rectify them or mitigate them.

A report should be produced covering the above-mentioned aspects. This should be contained in a central knowledge register with lessons learned incorporated into new ERPs.

5.3. Maintain ERP Documentation

The ERP will be updated annually, or when a significant business change occurs, and should be maintained as illustrated in Figure 8.

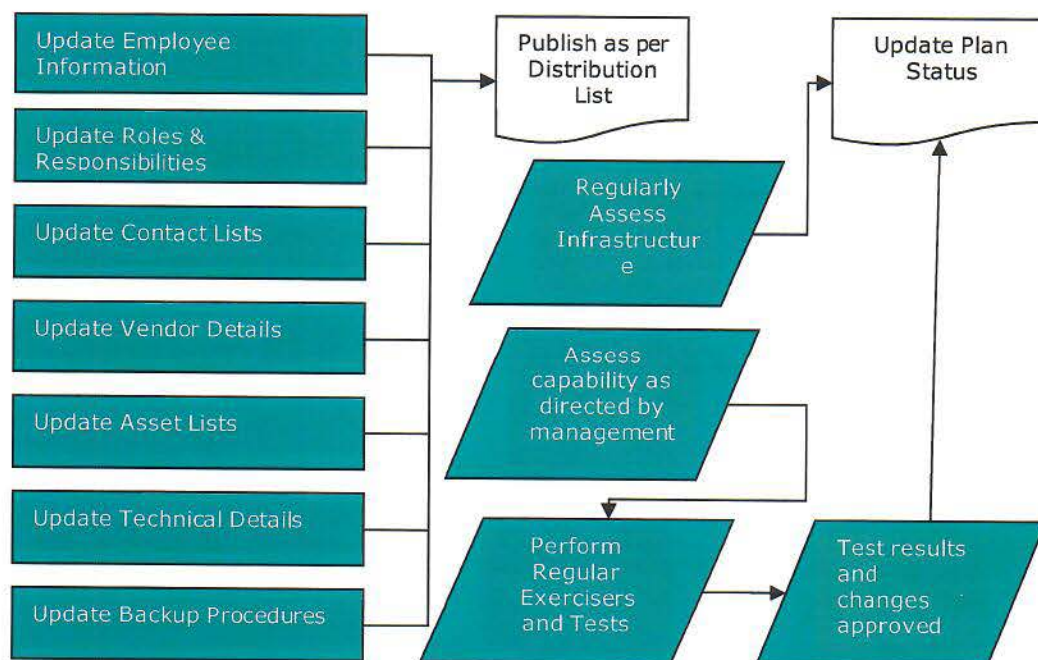


Figure 8: Maintain ERP Documentation Activities

In order to ensure currency of the Disaster Recovery Plan, all changes and revisions must be processed through the Chancellor's Office. The Chancellor will review the plan as part of the ERP testing process. On an on-going basis, the Chancellor or his/her designee will:

- periodically assess the conditions, status, capabilities and availability of backup computers, PCs, LAN, telecommunication configurations, and the facility
- perform special studies requested by the Management Team to improve the efficiency of equipment and recovery procedures
- prepare periodic status reports for the Management Team
- coordinate emergency recovery tests and prepare test results and recommendations for plan improvement
- maintain and distribute this plan.

5.4. Command CENTER Operations

The command CENTER(s) will be the physical *office(s)* that will be used in the event of a major disaster, the place where staff and vendors will first gather to establish the direction for dealing with the disaster at hand. Setting up and operating the command CENTER is the responsibility of the Management Team Leader, with activities as shown in the figure below. Depending on the situation and/or projected timeline, the command center might not be one central physical location. The CMT leader may decide that the command center is virtual.

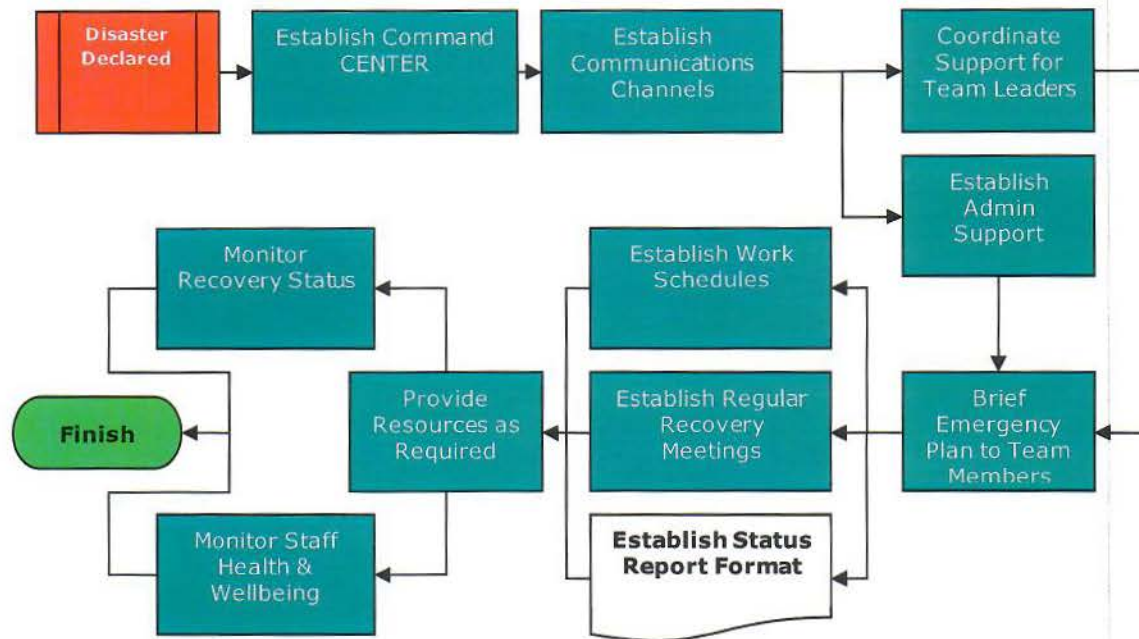


Figure 9: Command CENTER Activities

PART SIX – PROCEDURES

6.1. Management Team

6.1.1. Management Team Actions Overview

The Management Team is responsible for the entire disaster recovery process; from when the team is established until all services have been returned to the primary site or new location. The Management Team Leader or delegate, with input from relevant key personnel, has the exclusive authority to declare a Disaster and consequently activate this plan. See Section 1.1 – Authority to Activate this Plan.

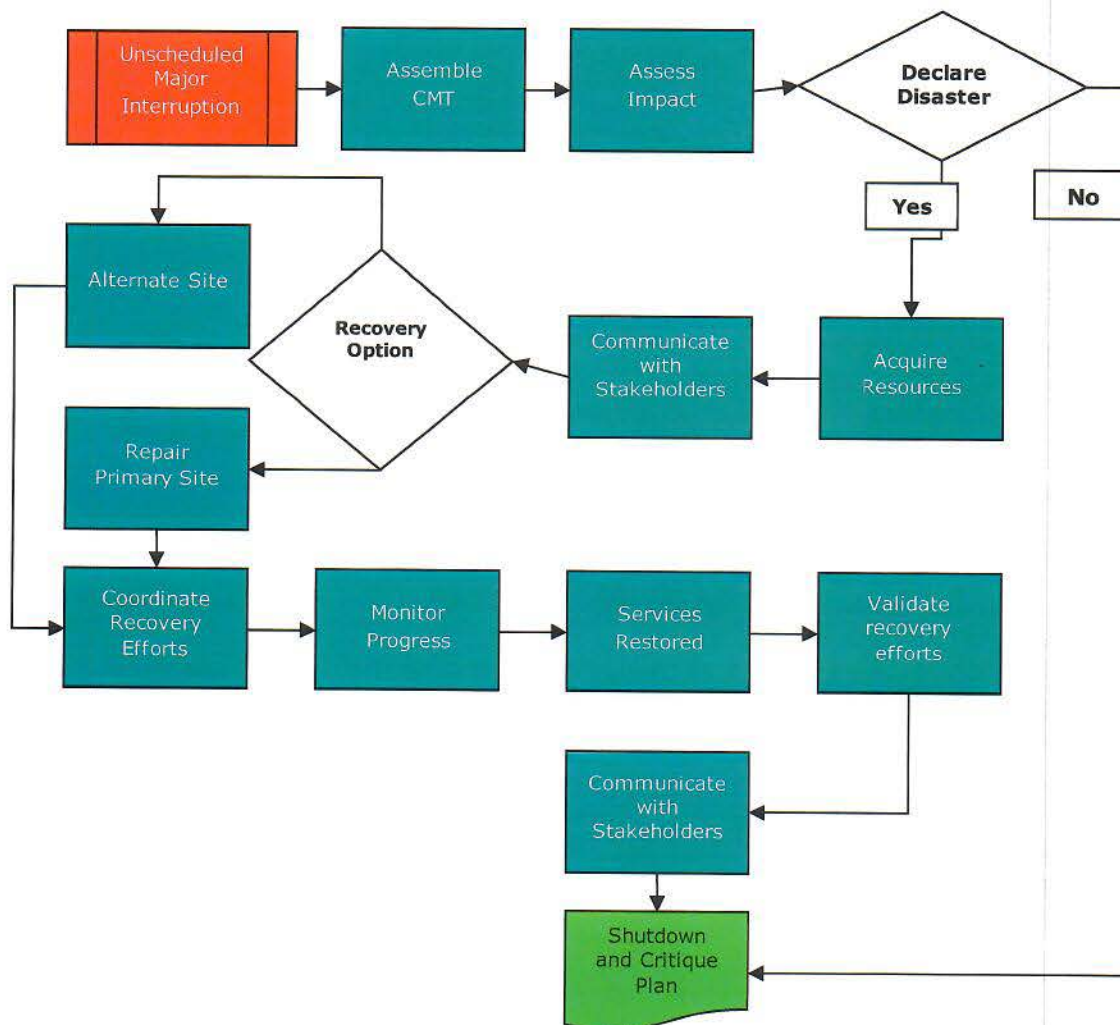


Figure 10: Management Team Activities

6.1.2. DR Management Team Actions

No.	ACTION STEP	WHO	TIME	RESOURCES	PROCESS TIME	COMMENTS
	<i>What do I have to do?</i>	<i>Who is responsible for the step to be completed?</i>	<i>How long will this take?</i>	<i>What additional resources are required?</i>	<i>When did I start and finish the action step?</i>	<i>What happened when I completed the action step?</i>
1.	Assemble Key Staff	Management Team Leader		Contact List		
2.	Assess Damage	Facility Management Team		Voice recorder		
3.	Decide Whether to Declare a Disaster or Not. If YES, go to Step 7.	Management Team Leader with input from the Management Team				
4.	Restore Functions at Primary Site	Each Team Leader				
5.	Debriefing of the Recovery	Management Team Leader				
6.	Finish	If Disaster alert is at stand down				
7.	DECLARE A DISASTER Initiate recovery to alternate site	Authorized individuals named in the Management Team				
8.	Acquire Equipment and Supplies	Management Team Leader				
9.	Communicate with Groups and coordinate recovery	Management Team Leader				
10.	Build New or Rebuild Primary Site	Management Team Leader				
11.	Monitor Progress	Management Team Leader				
12.	Move to New or Rebuilt Primary Site	Management Team Leader				
13.	Discontinue Use of Alternate Site	Management Team Leader				
14.	Debrief of Plan	Management Team Leader				
15.	Finish					

6.2. Facility Team

6.2.1. Facility Team Actions Overview

Prior to activating the facility team, the designated Facility Team leader should remain close to the scene of the disaster to help direct Emergency Services personnel. If evacuation is necessary, all personnel should immediately proceed to the pre-determined location, well clear of the building. A head count must be taken there to ensure that no one has been left behind, including visitors, contractors, etc. If there have been any injuries, immediately identify those people who can offer medical help, such as first aid.

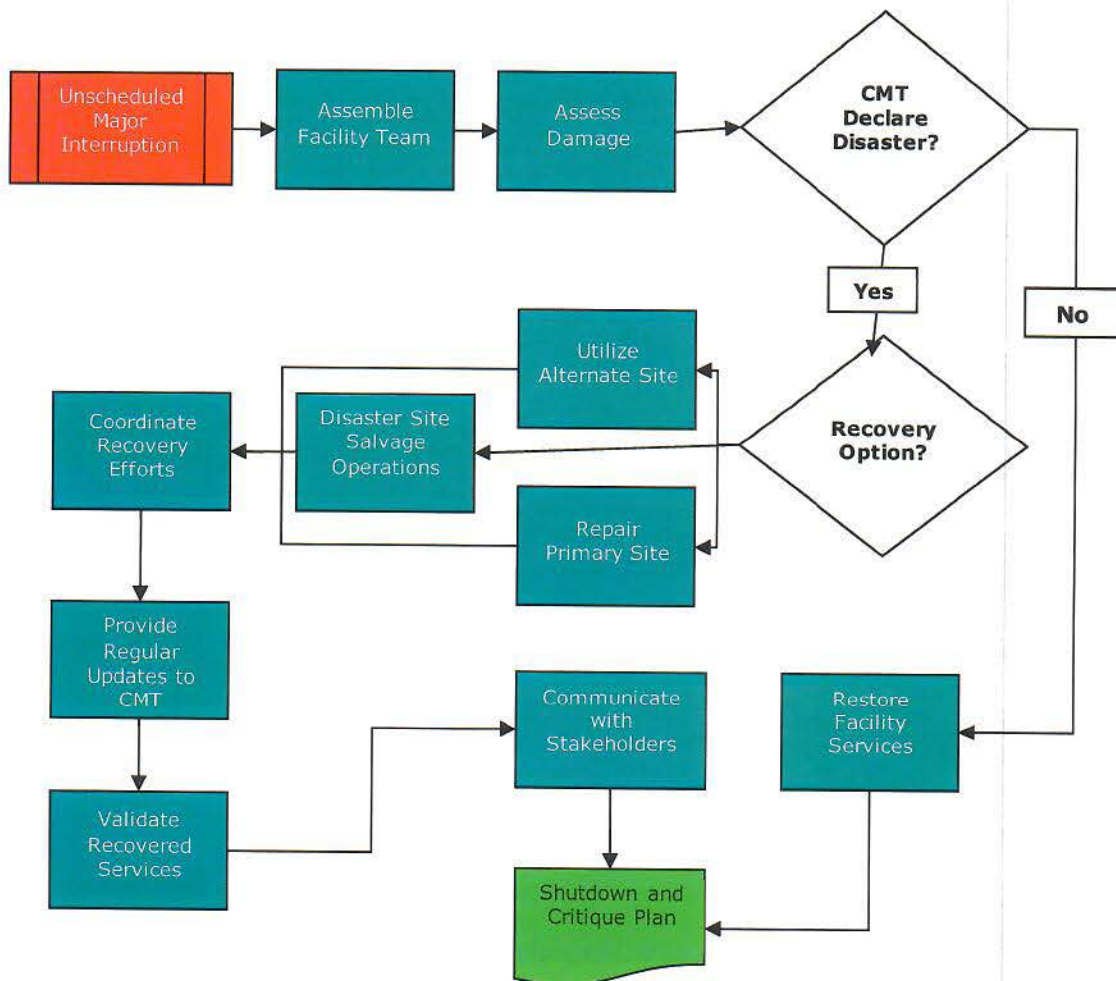


Figure 11: Facility Team Action Process

6.2.2. Facility Team Actions

	ACTION STEP	WHO	TIME	RESOURCES	PROCESS TIME	COMMENTS
	<i>What do I have to do?</i>	<i>Who is responsible for the step to be completed?</i>	<i>How long will this take?</i>	<i>What additional resources are required?</i>	<i>When did I start and finish the action step?</i>	<i>What happened when I completed the action step?</i>
1.	Activate Facility Team	Management Team Leader		Contact List		
4.	Disaster Site Evaluation & Salvage	Facility Team Leader				
5.	Build New or Rebuild Primary Site. <i>If decision is to build a new primary site, go to Step 12.</i>	Facility Team Leader				
6.	Plan Primary Site Rebuild	Facility Team Leader				
7.	Hold Recovery Status Meeting	Management Team Leader				
8.	Coordinate Move to Primary Site	Facility Team Leader				
9.	Discontinue use of alternate location	Facility Team Leader				
10.	Deliver plan critique	Facility Team Leader				
11.	Finish	Management Team Leader				
12.	Assist Alternate Site selection and Move	Facility Team Leader				
13.	Coordinate Move to New Primary Site	Facility Team Leader				
14.	Discontinue use of alternate location	Facility Team Leader				
15.	Deliver Critique of ER Plan	Facility Team Leader				
16.	Finish					

6.3. Recovery Team

6.3.1. Recovery Team Activities Overview

This section contains the procedures to be followed by the Recovery Team. The Recovery Team includes the hardware, software, and communications experts who travel to the alternate site. The Recovery Team restores the software and data onto an alternate-computing platform, and restores communications from that platform back to the users.

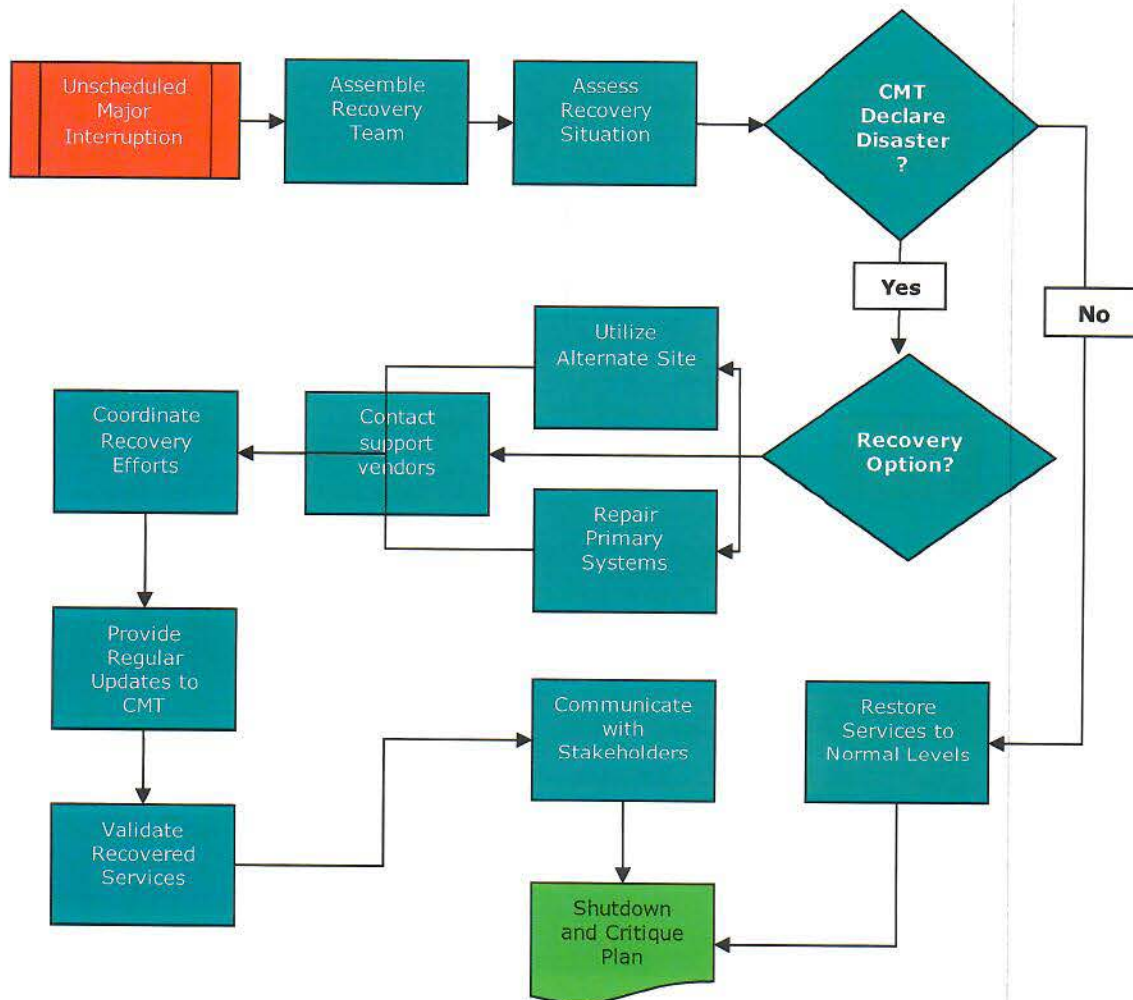


Figure 12: Recovery Team Activities

6.3.2. Recovery Team Actions

	Action Step	Who	Time	Resources	Process Time	Comments
	<i>What do I have to do?</i>	<i>Who is responsible for the step to be completed?</i>	<i>How long will this take?</i>	<i>What additional resources are required?</i>	<i>When did I start and finish the action step?</i>	<i>What happened when I completed the action step?</i>
1.	Activate Recovery Team	Management Team Leader		Contact List		
2.	Disaster Declared? If yes, go to Step 7.	Management Team Leader				
3.	Rebuild Primary Site	Facility Team Leader				
4.	Restore Operating Systems/Applications as Needed	Recovery Team Leader				
5.	Restore Data Communications	Recovery Team Leader				
6.	Critique Plan – Finish	Recovery Team Leader				
7.	Build Alternate Site – Transfer Operations	Recovery Team Leader				
8.	Restore Operating Systems/Applications	Recovery Team Leader				
9.	Restore Data Communications	Recovery Team Leader				
10.	Start Production Operations as Needed	Recovery Team Leader				
11.	Coordinate Move to New/Rebuilt Primary Site	Management Team Leader				
12.	Deliver Critique of DR Plan	Recovery Team Leader				
13.	Finish					

APPENDIX A – CONTACT LIST

Nunez Community College Management

Position	Name	Phone	Cell
Chancellor	Tina Tinney	504-278-6482	504-723-2621
Vice Chancellor of Education, Training, and Student Success	Cherie Kay LaRocca	504-278-6273	985-634-3376
Assistant Vice Chancellor of Education, Training, and Student Success	Leonard Unbehagen	504-278-6436	504-439-0662
Chief Financial Officer	Tai Nguyen	504-278-6474	504-495-5590
Associate Vice Chancellor of Institutional Advancement	Katherine Lemoine	504-278-6491	504-382-2090
Interim Executive Director of Strategic Engagement and Human Capital	Jason Leader	504-278-6256	985-373-8089
Director of Accounting and Budget	Dana Littlepage	504-278-6483	985-710-0674
Dean of Strategic Enrollment and Student Success	April Lavergne	504-278-6425	985-634-1532
Director of Communications	Jason Browne	504-278-6421	504-717-0508
Director of Facilities Management	Randy Hartzog	504-278-6373	985-705-1649
Director of Information Technology	Jason Hosch	504-278-6280	985-788-8644
Dean of Instruction	Reggie Poche	504-278-6277	504-273-9837
Dean of Nursing and Allied Health	Mary Fernandez	504-278-6418	985-634-1532

Facility Team

Position	Name	Phone	Cell
Director of Facilities Management	Randy Hartzog	504-278-6332	985-705-1649

Recovery Team

Position	Name	Phone	Cell
Director of Information Technology	Jason Hosch	504-278-6280	985-788-8644
Information Technology Analyst	Chris Hintzen	504-278-6281	512-663-5653

Disaster Recovery / Salvage Vendors

Company / Position	Name	Phone	Cell
St. Bernard Sheriff's Office	Sheriff Pohlmann	504-278-7685	504-583-3373
Fire/Emergency		911	
St. Bernard Parish/Emergency Mgmt.	Colonial David Dysart	504-278-4267	
Entergy	Ann Johnson	504-840-2672	504-884-5955
Securance (fire alarms)	Blake Gaudet	504-360-2423	504-462-0432
OTM/Telephones		225-342-7762	
Sewer & Water Board		504-271-1681	
Office of Risk Management	Jo Campbell (Team Lead)	225-368-3416	Jo.Campbell@sedgwich.com
Office of Risk Management	Carmen Turner	210-332-1603 ext. 21603	carmen.turner@sedgwick.com

Key Vendor Contact

Company / Service	Name	Phone	Cell/Email Addresses
Dell (Computers)	Shruti Agarwal	512-725-0429	shruti.agarwal@dell.com 225-907-4783
SHI	Allison Roy		Allison_roy@shi.com
CDWG	Juan Villa	312-705-4525	juanvil@cdwg.com
A-1 Signs (Marquee)	Steve Barnett	504-947-8381	504-952-0338
LONI (Network Operations)		317-278-0149	noc@loni.org
LONI	Lonnie Leger	225-341-1832	Lonnie@lsu.edu
LONI	Phillip Stott	504-236-8466	Pstott@lsu.edu
ManageEngine (ADSelfService)		888-720-9500	support@adselfserviceplus.com
Cox	Eugene 'Butch' Holmes	504-258-6352	Eugene.holmes@cox.com
Cox	Larry Hattier	504-358-6029	504-313-2843
Cox	Herb Seals	225-930-2433	Herbert.seals@cox.com
Cox	Customer	800-699-8175	Use this one first.

	Services		
Campus Suite	Support		helpdesk@campussuite.com
Extreme	GTAC	800-872-8440	
Extreme	Brian Rupiper	208-769-9920	208-819-0823
FP & C	Alan Antoine	504-568-2414	
Venyu	Support	866-978-3698	
LiveHelpNow	Support	877-548-3001	livehelpnow.net Use Chatbot for Service
Howard	Amanda Phippen	301-399-5827	aphippen@howard.com
Netop	Joudan Lopez	971-712-7350	jolu@netop.com
SCW	William Christian	770-579-8927	william.christian@m.scw.com
Benecom	Joe Fall	504-254-1441	504-415-9501
Benecom	Dustin Benedict	504-254-1441	504-908-0664
Television Stations	Telephone#	Fax#	Email Address
WWL-TV Channel 4	504-529-4444 General Information	504-529-6472	www.wwltv.com
WWL-TV News	504-522-4404 Action Line		
WDSU News 6	504-679-0600 Main Line	504-679-0733	www.wdsu.com
WVUE Fox 8	504-486-6161	504-483-1543	Fox9news@wvue.emmis.com
WGNO 26	504-619-6363	504-619-6332	www.abc.26.trb.com
WNOL TV CW 38	504-525-3838 Main Line	504-619-6332	www.neworleanscw38.trb.com
Radio Stations			
WWL-AM 870	504-593-6397 1-866-889-0870	504-593-2099	www.wwlnewsroom@ yahoo.com
CITADEL	504-581-7002		
ENTERCOM	504-593-6376		
CLEAR CHANNEL	504-679-7300		

Key Stakeholder Contacts

Company Name	Name	Phone	Cell
State Representative	Ray Garofalo	504-277-4729	
State Senators	Sharon Hewitt or JP Morrell		
St Bernard Parish School Board	Doris Voitier	504-301-2000	
St Bernard Parish President	Guy McInnis		

System Contacts

LCTCS	Name	Phone	Email Address
Louisiana Community & Technical College System 265 S. Foster Dr., Baton Rouge, LA 70806	Joe Marin	225-922-1635 Office	jmarin@lctcs.edu

APPENDIX B – SYSTEM RECOVERY REQUIREMENTS

Recovery Priority for IT Systems

Application / Data	Processes Supported	Priority	Recovery Timeframe
Server, legacy archive, minimum two computers, switch	Internet	1	24 hours
Establish temporary e-mail accounts, possibly additional website	Human Resources, External contact	1	48 hours
Assess onsite damage (if access is available)	Restoration of site	2	1 week
Begin site restoration or continued expansion of remote site(s)	All	3	1 - 2 weeks

APPENDIX C – RETRIEVAL OF OFF-SITE BACKUPS.

Introduction

Note: Availability of backup data is critical to the success of disaster recovery. Backup and restore processes are conducted on a daily and weekly basis with an integrity test of those backups conducted monthly.

This procedure must be used in the event of an actual disaster at the Chalmette campus, to retrieve some or all of Nunez Community College data stores from the remote facility.

Procedure

Data backups are stored on a cloud-based Dell appliance with all data being secured in the cloud off site. The Information Technology Department will initiate a recovery download from Dell in the event on premise servers are destroyed; the Information Technology Analyst will also possess the same data restore abilities should the Director become incapacitated. Once the data has been successfully restored, it will be disseminated to the appropriate departmental reps or used to rebuild any destroyed systems thus restoring functionality on campus.

APPENDIX D – SYSTEM NOTIFICATION

The Louisiana Community and Technical College System (LCTCS) is the governing board for Nunez Community College.

Notify Louisiana Community and Technical College System (LCTCS) of Disaster

All system institutions must notify the LCTCS as soon as possible and no later than **24 hours** after experiencing a major disruption that has the potential to material impact depositors and/or policy holders.

Contact Procedures:

- Information Hotline: 225-922-1635
- Postal address: 265 S. Foster, Baton Rouge, LA 70806
- Email: jmarin@lctcs.edu

APPENDIX E – BUSINESS IMPACT ANALYSIS PROCESS

Process

The Nunez Community College Business Impact analysis (BIA) process involves identifying all critical business functions, resources and infrastructure of the business and assessing the impact of a disruption on these.

Outcomes

As a result, Nunez Community College determines the potential financial, legal, reputation and other consequences if the critical business functions, resources and infrastructure are unavailable for a given period of time.

The BIA determines the maximum tolerable downtime during which the business could not operate without its critical business functions, resources and infrastructure. The priority and timeframes assigned for the recovery of critical business functions, resources and infrastructure are in turn decided.

Whole of business approach

The BIA covers all units of the business to ensure a whole of business coverage. Nunez Community College Management is tasked with ensuring that adequate representation and involvement from all business units when undertaking the BIA.

Frequency

Nunez Community College will conduct a BIA every two years, or as a result of significant business change.

APPENDIX F – COMMAND CENTER DETAILS

Command Center Location

Nunez Community College (NCC) and Central Louisiana Technical Community College (CLTCC) entered into a MOU [link signed MOU] to allow NCC to use CLTCC campus as an alternative command center after an emergency/disaster.

- Address: 4311 S MacArthur Dr, Alexandria, LA 71302,
- Phone: 318-487-5443

Key Central Louisiana Technical Community College Contacts:

- Jimmy Sawtelle, Chancellor, ext 1160, jsawtelle@cltcc.edu
- Amanda Cain, Vice Chancellor of Finance and Administration, ext. 1161, amandacain@cltcc.edu

Command Center Checklist

Activity	Checked OK?
<ul style="list-style-type: none"> • Establish a command CENTER work location for each activated recovery team, staff department and vendor. 	
<p>Ensure that adequate furniture, fixtures, PCs, telephones, supplies and space are provided for each group. Use the Resource Checklist at the end of this section.</p>	
<p>Prepare signs that identify the room or work area assigned to each group.</p>	
<ul style="list-style-type: none"> • Establish incoming and outgoing communication channels. 	
<p>Assign specific telephones to be used for incoming and outgoing calls.</p>	
<p>Continue department notification activities until all personnel have been reached.</p>	
<p>Assign personnel to monitor the telephones designated for incoming calls.</p>	
<p>Inform the company telephone operators to direct all return calls to the assigned extension(s) at the command CENTER.</p>	
<ul style="list-style-type: none"> • Coordinate staff department support with team leaders during the recovery. 	
<p>Meet with security representative to review the need to assign security personnel to secure the damaged business site and the recovery operations site(s). Depending on the nature of the disaster, tighter than normal security for personnel and property may be required.</p>	
<p>Request that admittance be restricted to only authorize personnel who have proper identification (company ID badge, etc.).</p>	

Activity	Checked OK?
Work with the Facility Team to identify equipment requirements and arrange for the Purchasing Department representative to provide the following:	
Heavy duty copy machines	
Miscellaneous paper, pencils pens, etc.	
<ul style="list-style-type: none"> • Ensure all third-party vendors are contacted and notified of the situation. 	
<ul style="list-style-type: none"> • Brief the recovery plan to core recovery team members. 	
<p>The intent is to review the organization and work to be done, to clarify responsibilities and to answer any questions.</p>	
<ul style="list-style-type: none"> • Establish status reporting processes and formats. 	
<ul style="list-style-type: none"> • Create the following status charts, using flip charts or other media, for display at the command CENTER: 	
Information Status Display	
General Message Board	
Personnel Accommodation Board.	
<ul style="list-style-type: none"> • Establish regular recovery meetings 	
Keep all recovery team personnel informed of the recovery progress.	
Advise recovery team leaders.	
Arrange and organize a meeting place.	
Record minutes of the meetings.	
Have minutes typed, obtain approval, and distribute them.	
<ul style="list-style-type: none"> • Establish work schedules for 24-hour coverage. 	
Align the off-shift work effort with the Recovery Time Objective.	
<ul style="list-style-type: none"> • Continue to evaluate the level of people and resources and add or subtract as needed. 	
HR and Purchasing are the focal points for people and resources.	
<ul style="list-style-type: none"> • Monitor personnel for signs of fatigue. 	
<p>Sufficient rest is required to maintain an efficient recovery operation. For health and efficiency reasons, no recovery personnel should work excessive hours without an eight-hour rest period.</p>	

Table 4: Command CENTER Checklist

Resource Checklist

The command CENTER should be well equipped with extensive communications facilities. Communications are highly critical when rescue and medical care are primary and time is of the essence. This is particularly true when families of key personnel are threatened. Without effective mass communications, your key personnel may leave to be with their families.

In addition to the communications facilities mentioned above, the command CENTER should be outfitted with, or have ready access to food, clothing, sleeping accommodations, and other supplies needed to manage the recovery effort (a checklist is provided in Table 5).

Resource	Checked OK?
Telephones	
Inbound and outbound phone lines (2 are recommended)	
Telephone directories	
Television set	
Camera/Camcorder	
Copy machine	
Fax machine	
Portable light	
Radio/Tape Recorders	
Whiteboard	
Overhead projector	
Chart to record recovery milestones	
PCs and printers	
Letters of credit	
Medical supplies	
Food/Water	
Cooking facilities	
Sleeping accommodations	
Office supplies	
Recovery Records	
This recovery plan	
Maps and building plans	
Emergency action logs	
Floor plan/specifications of building(s)	

Table 5: Resource Checklist

APPENDIX G – IT RECOVERY PROCEDURES

IT Disaster Recovery Plan

Elaine P. Nunez Community College
Department of Information Technology

Primary Focus of Plan:

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples the College's central computer systems operated by the Department of Information Technology. The intent is to restore mission critical operations as quickly as possible with the latest and most up-to-date data available.

The techniques for backup and recovery used in this plan do NOT guarantee zero data loss. Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup uploads. Significant effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point of the disaster forward.

Individual users and departments will need to develop their own disaster recovery plans to cope with the unavailability of the computer systems during the restoration phase of this plan and to cope with potential data loss and synchronization problems.

Primary Objectives of this Plan:

Present an orderly course of action for restoring critical computing capability to the Nunez Community College campus within the shortest amount of time possible after initiation of the plan. Provide information concerning personnel that will be required to carry out the plan.

Section 1: Overview of the Plan

This plan is designed to aid in the recovery from a disaster that destroys or severely cripples the computing resources at Nunez Community College located at 3710 Paris Road, Chalmette LA 70043 and possibly at other critical campus facilities.

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, USB drives, etc) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

At the same time, a survey of the disaster scene is conducted by appropriate personnel to estimate the amount of time required to put the facility (in this case, campus buildings and utilities) back into work order. A decision is then made whether to use a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

Restore data from Backups

Data recovery relies entirely upon the use of backups stored in locations off-site. Backups can take the form of a storage appliance, offsite backup's transmissions, external storage media or CDROMs. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of mission critical applications and data from the backup transmissions is conducted. Individual application owners may need to be involved at this point, so teams are assigned for each major application area to ensure that data is restored properly.

Restore Applications Data

It is at this point that the disaster recovery plans for users and departments must merge with the completion of the Office of Information Technology plan. Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, the College computer systems can reopen for business. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

Move Back to Restore Permanent Facility

If the recovery process has taken place off-site, physical restoration of the primary site (or an alternate facility) will have begun. When the facility is ready for occupancy, the systems assembled off-site are to be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to the recovery off-site.

Disaster Risks and Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created.

1: Fire

The threat of fire is very real and poses the highest risk factor of all the causes of disaster mentioned here. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. The computers within the facility also pose a quick target for arson from anyone wishing to disrupt operations.

A. Preventative Measures

Fire Alarms and alert system

B. Fire Extinguishers

Hand-held fire extinguishers are required in visible locations throughout the building. Staff is to be trained in the use of fire extinguishers.

C. Training

Staff is required to undergo training on proper actions to take in the event of a fire. Staff is required to demonstrate proficiency in period, unscheduled fire drills.

D. Recommendations

Regular review of the procedures should be conducted to ensure that they are up to date. Unannounced drills should be conducted by an impartial administrator and a written evaluation should be produced for the department heads housed in the building. Regular inspections of the fire prevention equipment are also mandated. Fire extinguishers are periodically inspected as a standard policy.

2: Flood

The College is located in an area vulnerable to flooding. This factor coupled with the chance of a storm that drops large amounts of rain in the Chalmette area create the threat of flooding. Flood waters penetrating the server room can cause substantial damage. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections. Of course, the presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel.

A. Preventative Measures

Essential computer equipment is located at the highest possible level. In regards to the server and switching cores, both areas are located on the 2nd floor of the AST building as it provides not only elevation from possible storm waters but also adds an additional level of protection from possible high winds. All communication/switching closets are located on the 2nd floor of each campus building (where possible); in locations in which there is no second floor, switches and protective UPS devices are mounted as high as possible in their racks (typically above 5 feet).

B. Recommendations

All primary communication housing locations need to be inspected on a regular basis to ensure the threat of flooding from internal or external causes is not present. Switching and core locations are inspected by IT personnel on a regular basis.

3: Hurricanes and Tornados

As Nunez Community College is situated in an area prone to heavy thunderstorms, hurricanes and tornados spawned by those storms, damage due to these conditions is a very real possibility. A hurricane or tornado has the potential for causing the most destructive disaster to our facility.

A. Preventative Measures

The server core as well as the primary switching core along with all switching and communication devices are stored in designated closets on the 2nd floor of each campus building; this not only provides elevation protection from flood waters but also adds a layer of protection from high winds as these rooms are reinforced. In areas where a 2nd floor is not available for switching/communications housing, these devices are mounted as high as possible in their storage racks, typically 5 feet and above (if possible).

In addition, all data backups are conducted by a cloud-based backup system that is not on premises; backups are conducted and transmitted daily to stay current. In the event of an impending weather system that may cause damage to the network, a backup is ran and transmitted prior to shutting down the servers as a precaution.

B. Recommendations

The Office of Information Technology should have large tarpaulins or plastic sheeting available in the server room area ready to cover sensitive electronic equipment in case the building is damaged.

4: Computer Crime

Computer crime is becoming more of a threat with the continual advancement of hacking tools, malware and ransom are (to name a few). Computer crime “usually” does not affect hardware in a destructive manner (however this threat is becoming more real each year). The threat of computer crime can originate from external sources or attacks for from within by a disgruntled employee or student.

A. Preventative Measures

The server room as well as the primary switching core and all subsequent data/communication closets are locked at all times; access to these locations is strictly limited to IT personnel and necessary maintenance staff with an IT escort with prior authorization.

All campus wide computing systems use a combination of anti-virus, anti-ransomware and anti-spyware detectors to prevent unauthorized access from external sources; all users also possess unique logins that limit their ability to access data across the campus network (passwords for these logins are changed on a regular basis).

The campus also utilizes several firewalls and anti-hacking hardware, software and monitors to protect against external (or internal) data breaches by unauthorized personnel; all networking traffic is monitored by several devices that IT staff monitor regularly for issues.

Data servers are backed up on a regular basis several times a week to ensure a speedy recovery is possible in the event an incident occurs. These backups are tested on a monthly basis for functionality and adjustments made (if necessary).

B. Recommendations

Continue to improve security functions on all platforms; strictly enforce policies and procedures when violations are detected.

Users will undergo quarterly security training in conjunction with LCTCS policy and best practices; users are also required to change their system passwords at regular intervals.

IT will continue to implement security devices and protocols to combat that ever changing electronic threats to the campus.

Section 2: Disaster Planning

In order to facilitate recovery from a disaster which destroys all or part of the server room, certain preparations have been made in advance. This document describes what has been done to lay the way for a quick and orderly restoration of the facilities that the Office of Information Technology Operates.

The following topics are presented in this section:

- A. Disaster Recovery Planning
- B. Recovery of Facility
- C. Replacement of Equipment
- D. Backups

A. Disaster Recovery Planning

The overall plan of which this document is a part is that which the Office of Information Technology will use in response to a disaster. The extent to which this plan can be effective, however, depends on disaster recovery plans by other departments and units within the College.

For instance, if the Administration Building were to be involved in the same disaster as the Office of Information Technology, the functions of a Business Unit could be severely affected. Without access to the appropriate procedures, documents, vendor lists, and approval processes, the Office of Information Technology recovery process could be hampered by delays while that unit recovers.

Every other business unit within the College should develop a plan on how they will conduct business, both in the event of a disaster in their own building or disaster at the Office of Information Technology that removes their access to data for a period of time.

Those business units need a means to function while the computers and network are down, plus they need a plan to synchronize the data that is restored on the central computers with the current state of affairs. For example, if an Office is able to function while the central computers are down, the data will have to be re-entered into the central computers when they return to service. Having a means of tracking all data changes while the central computers are down is extremely important.

B. Recovery Facility

If a central facility operated by the Office of Information Technology is destroyed in a disaster, repair or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at an alternate site.

Alternate recovery site is an area where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired or rebuilt.

It must have adequate space to house the hardware, with some office space available for operating and technical personnel. It requires good connectivity to the campus fiber optic network.

C. Replacement Equipment

The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configurations. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. The Recovery Team will have the expertise and resources to work through these problems as they are recognized. Although some changes may be required to the procedures documented in the plan, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process.

D. Backups

In the event of a disaster, data must be restored from a backup copy that was not affected by the disaster.

Periodic backups of server systems are stored both on an onsite appliance as well as at a secure offsite repository. The offsite location is fully accessible via internet connection by the Director of Information Technology and the Information Technology Analyst.

Backups are conducted on a daily and weekly basis and checked monthly for functionality.

Section 3: Initiation of Recovery Procedures

The Office of Information Technology will obtain the most recent data backup and restore on campus; if the onsite appliance cannot be used, the backups will be downloaded from the offsite storage location.

All patches and hot fixes necessary to bring the servers up to current compliance after restoration will be applied. Servers are to be restored **IN THE FOLLOWING ORDER:**

Server Count: 15

DCSRV2(Virtual):

O/S-Windows Server 2016

Function- Domain Controller, DNS/DHCP

DCSRV4(Virtual):

O/S-Windows Server 2016

Function- Domain Controller, DNS/DHCP

DCSRV6(Virtual):

O/S-Windows Server 2016

Function- Domain Controller,

Photon-machine (Virtual):

O/S-Linux VMware vCenter application server

Function- vSphere web server

MDT (Virtual):

O/S-Windows Server 2019

Function- SCCM, KMS license server

ADSelfservice (Virtual):

O/S-Windows Server 2019

Function- Password reset tool

SHAREDSRV1 (Virtual):

O/S-Windows Sever 2016

Function-Departmental File Storage, Historical Archive

PRNTRSRV1 (Virtual):

O/S-Windows Server 2016

Function-Network printing control

3M (Virtual):

O/S-Windows Server 2016

Function-Medical Billing and Coding software application server

TBCSRV (Virtual):

O/S-Windows Server 2016

Function-licing server for Geospatial

Solidworks (Virtual):

O/S-Windows Server 2016

Function- licing server for Solidworks

Magicinfo (Virtual):

O/S-Windows Server 2016

Function-TV's web application controller

NAC (Virtual):

O/S- Linux

Function- WIFI monitoring application

NAC2 (Virtual):

O/S- Linux

Function- WIFI monitoring application

Netsight (Virtual):

O/S- Linux

Function- WIFI monitoring application

Server Physical Information:

Control Server for Virtual Servers

PowerEdge VRTX Chassis

- 1. 74 TB Storage**

- a. 7 * (4 TB) SSD MZILT3T8HALS0D3
 - b. 7 * (7 TB) SSD MZILT7T6HALA0D3
2. 3 * PowerEdge M640
- a. CPU Cores: 12 CPU @ 2.30GHz
 - b. Processor Type: Intel(R) Xeon(R) Gold 5118
 - c. Ram: 510 GB
 - d. System Type: 64 Bit (For Virtual OS)
 - e. OS for Core: VMware ESXI, 6.7.0

Disaster Notification List:

Jason Hosch

IT Director

On Campus: Ext 280 Cell: 985-788-8644

Chris Hintzen

IT Analyst

On Campus: Ext 281 Cell: 512-663-5653

APPENDIX I – MEDIA CRISIS MANAGEMENT

Procedures for Dealing with the Media

When a crisis occurs, media may call staff or you. In the event of calls occurring, please follow the procedures below.

- Take down the name, organization and contact numbers for the media person calling and advise them that “a spokesperson will be in touch with them as soon as possible.”
- If pushed for details or further information, politely tell them that “a spokesperson for the company will be available to answer all queries and will call back as soon as possible.”
- When the media call they will be both very nice and unassuming or very abrupt and demanding. Both methods are used to either secure information in a friendly, non-threatening environment or the opposite, whereby they use their seeming authority to demand information. Journalists like answers and they want them straight away.
- Be polite, even identify with their need for information but acknowledge to them that you are not in a position to assist them. However, you will ensure that “a company spokesperson will be calling them back.”
- It is important to clearly identify the publication and contact details, both work and cell phone for a quick response.
- Be aware that the caller may not clearly identify himself or herself as a media person.
- Journalists will often ring and just ask for the mobile number of the Chief Executive or Head of Operations. **Do not give out these names or contact numbers to the caller.** In this situation the response needs to reinforce the message that “a spokesperson for the company will call back as soon as possible.”
- Once media calls have started to come in and you have journalists’ names and numbers, it is vitally important that the information is handed immediately to the Crisis Management Team Leader. Do not give out names or contact numbers to the caller. If media calls are left unanswered for more than one hour, this will build tension and create further issues.
- The Crisis Management Team Leader will be the KEY contact point for all media enquiries. However, media should not be referred directly to this person. It is important that you take down their details and reinforce that “a spokesperson for the company will be in touch as soon as possible.”
- It is now up to the Crisis Management Team Leader and Crisis Management Team to formulate responses to the media and ensure that those responses are clear, direct and quickly distributed to the media, in conjunction with other authorities that may be involved in the incident (i.e., Police, Emergency Services, etc.)

APPENDIX J – EVENT LOG

ELAPSED TIME SINCE START (hh:mm)	BCP Ref.	RECOVERY TASK	TEAM	ACTUAL START TIME	ACTUAL END TIME	COMMENTS/ PROBLEMS	SIGN OFF

